



CLOUD OPERATIONS BEST PRACTICES & RESOURCES GUIDE



A PRODUCT BY **IT MODERNIZATION**
OFFICE OF TECHNOLOGY POLICY

TABLE OF CONTENTS

 Acknowledgement4
 Purpose5
 Audience.....	.5
 Objectives.....	.5
 Executive Summary6
 Introduction.....	.7
Principles.....	.8
Assumptions9
How this Guide is Organized.....	.9
Cloud Operations versus Traditional IT Operations11
Cloud-Based Resources Change Responsibilities13
 Leadership15
Cloud Operations Strategy15
Planning16
Current State Assessment.....	.18
Organizational Change Management20
Organizational Design.....	.22
 Business Management26
Financial Management26
Cost Management.....	.31
Performance Management39
Capacity Management40
Quality Management.....	.41
Vendor Management.....	.44
Governance45
Portfolio Management & Rationalization50
Workforce Planning53
Sustainability55

 Security	56
Cloud and On-Premise Differences that Impact Security	58
Changing Agency Responsibilities	58
Customer Responsibility Matrix	59
Assessment & Authorization	59
Monitoring	63
Supply Chain Risk Management	64
Establishing Digital Trust	65
Secure Cloud Service Configurations	66
API Security	67
Encryption	68
Zero Trust	69
Getting Help from CISA	70
 Engineering	71
Target State	71
Provisioning & Deployments	74
Sustainment	79
 Conclusion	89
 Appendix 1: Assessing Readiness for Cloud Migrations	90
 Appendix 2: Capacity Planning Template	93
 Appendix 3: Sample Cloud RACI Chart	94
 Appendix 4: Typical Cloud Roles	103
 Appendix 5: Change Management Process and Questions to Support Cyber-Supply Chain Risk Management	106



ACKNOWLEDGEMENT

The General Services Administration gives thanks to the many experts who helped make this guide possible. They include the following agencies:

Census Bureau, Congressional Budget Office, Consumer Product Safety Commission, Consumer Protection Financial Bureau, Department of Agriculture, Department of Education, Department of Housing and Urban Development, Department of Interior, Department of Justice, Department of State, Farm Credit Administration, Federal Emergency Management Agency, Federal Reserve Board, Fish and Wildlife Service, Food and Drug Administration, Library of Congress, National Aeronautics and Space Administration, National Oceanic and Atmospheric Administration, National Security Agency, Nuclear Regulatory Commission, Office of Management and Budget, Pacific Northwest National Laboratory, Pension Benefit Guaranty Corporation, Securities and Exchange Commission, Transportation Security Administration, U.S. Air Force, U.S. Army, U.S. Marines, U.S. Navy, and the Veterans Administration.



PURPOSE

Provide best practices and resources to support agencies in developing and maintaining efficient and effective cloud operations.

AUDIENCE

Agency staff who are leading or supporting the implementation and management of cloud operations. This includes Program Managers, Project Managers, and Cloud Professionals.

OBJECTIVES

- Provide foundational components of cloud operations.
- Support implementation and maturation of cloud operations.
- Identify available resources to support an agency's cloud operations.



EXECUTIVE SUMMARY

This guide supports a federal agency's journey to optimize its cloud operations.

Whether purchasing new cloud services, migrating applications, or simply managing your current IT investments, your agency's ability to manage the cost, capability, security and quality of your cloud impacts how well it serves its mission and its stewardship of taxpayer dollars.

The overarching theme of this guide is that cloud operations fundamentally differ from traditional IT operations. This difference emerges in virtually every aspect of IT operations, including strategy, planning, budgeting, governance, monitoring, provisioning, and more.

A second theme focuses on the practices presented as part of a continuous effort to improve operations. There is no one-and-done, one-size-fits-all best practice. Instead, successful improvement in cloud operations will be incremental and repeated. Furthermore, these practices are often interconnected. For example, optimizing cloud resources will require capture and analysis of data (see [Cost Management](#)) to identify and correct overprovisioning (see [Optimization Practices](#)).

Your peers wrote this guide. Eighty-two subject matter experts across 31 federal agencies or component offices contributed to this effort. Through many working sessions, many Cloud and Infrastructure Community of Practice (C&I CoP) working group members shared their hard earned expertise to help federal agencies accelerate their learning and improve their cloud operations.

The guide is not a how-to or training document; it is not meant to be read cover to cover. Rather, it is organized to allow readers to quickly find the relevant best practices, useful resources, and agency templates on a specific topic of interest.

The C&I CoP working group hopes this information will prove useful in your efforts to create a mission-effective cloud environment.





INTRODUCTION

As more agencies decide to move their IT infrastructure to the cloud, they must address significant budget, planning, governance, and security issues to ensure their cloud operations safely, effectively, and efficiently deliver the planned services to their customers. Supporting the cloud efficiently and effectively necessitates a paradigm shift from traditional, on-premise IT operations and requires agencies to embrace new approaches, tools and frameworks.

This *Cloud Operations Best Practices and Resource Guide* provides an enterprise perspective for the many issues that IT professionals and managers should address. This document is not intended as a how-to guide, but rather a comprehensive overview of **key cloud operational areas**. Also, this document is not intended to be read cover to cover. It is designed to support the quick identification of a topic of interest and the associated practices and resources.

The contributors to this guide have focused on key areas, best practices, and meaningful references. Our effort is to ensure relevant resources are identified for further analysis rather than attempting to provide all the needed information in this document.

As a final note, the fast-changing nature of this industry puts any assembled work on a short lifecycle. The practices and references in this guide may be the best today, but tomorrow will certainly bring something better.

We welcome any feedback that you have for this document.
Please send any questions or comments to dccoi@gsa.gov.

PRINCIPLES

A motivating factor behind these recommendations is that **operating your cloud investment is fundamentally different from traditional on-premise or data center operations**. The principles outlined below are products of this thinking. And, while the category of activities, such as budgeting or governance, are often the same, agencies must evaluate and update their approach as necessary to reflect these new realities and realize optimal gains.

- **Outcomes Focus.** Carefully consider the total cost of ownership and the return on investment when assessing future investments (e.g., automation). Both financial and non-financial costs should be assessed as part of the business case.
- **Agility.** Capabilities like elasticity and scalability allow cloud infrastructure to grow and shrink based on demand. These types of changes can happen much more quickly than traditional operations (e.g., hours versus days/weeks), so long-standing practices for funding, governance, and monitoring may need updating to reflect this faster pace.
- **Automation.** Automating tasks is a key optimizer for cloud operations. Self-provisioning, for example, might leverage automation to efficiently create standardized resources that can be efficiently managed. However, agencies should never assume that automating any given operational task is justified. Automation may be less relevant for your agency depending on the maturity and scale of your cloud operations. Simply, the cost and effort of automating a task should be balanced against the expected benefits.



- **Continuous Improvement.** Transforming your agency IT to fully optimize cloud operations is a journey. Whether optimizing individual cloud resources or updating change management policies, an agency would likely benefit from making incremental changes across the spectrum of cloud operational activities and revisiting as needed. This includes both technical and non-technical processes.
- **Shared Responsibility.** With the cloud, agencies are no longer responsible for the physical infrastructure and, depending on the cloud solution, many other responsibilities typically associated with the traditional IT operations. Understanding these changing needs will impact key management areas for your agency.

ASSUMPTIONS

For this guidance, the term “cloud” is most accurately applied to those solutions that exhibit the five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. See [NIST 800-145 The NIST Definition of Cloud Computing](#).

While this guide is intended to represent the broadest overview of the cloud operations ecosystem, this guide focuses on Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) environments more than Software as a Service (SaaS).

Please note that this guide outlines concepts that can be applied to any IaaS vendor. Furthermore, terms within this document are not vendor-specific but may coincidentally be used by certain vendors. This is not a recommendation for any specific vendor. Agencies have the responsibility to evaluate and acquire cloud services based on their unique business and technical requirements.

HOW THIS GUIDE IS ORGANIZED

Cloud Operations (Cloud Ops) is the management of cloud-based infrastructure, applications, and services. For this guide, we will not address other important and related issues like cloud design. Rather, we will focus on the issues associated with operating and maintaining your cloud assets as well as provisioning new resources and migrating existing on-premise applications. These areas are Leadership, Business Management, Security, and Cloud Platform Engineering. See Figure 1, Important Knowledge Domains for Cloud Operations.

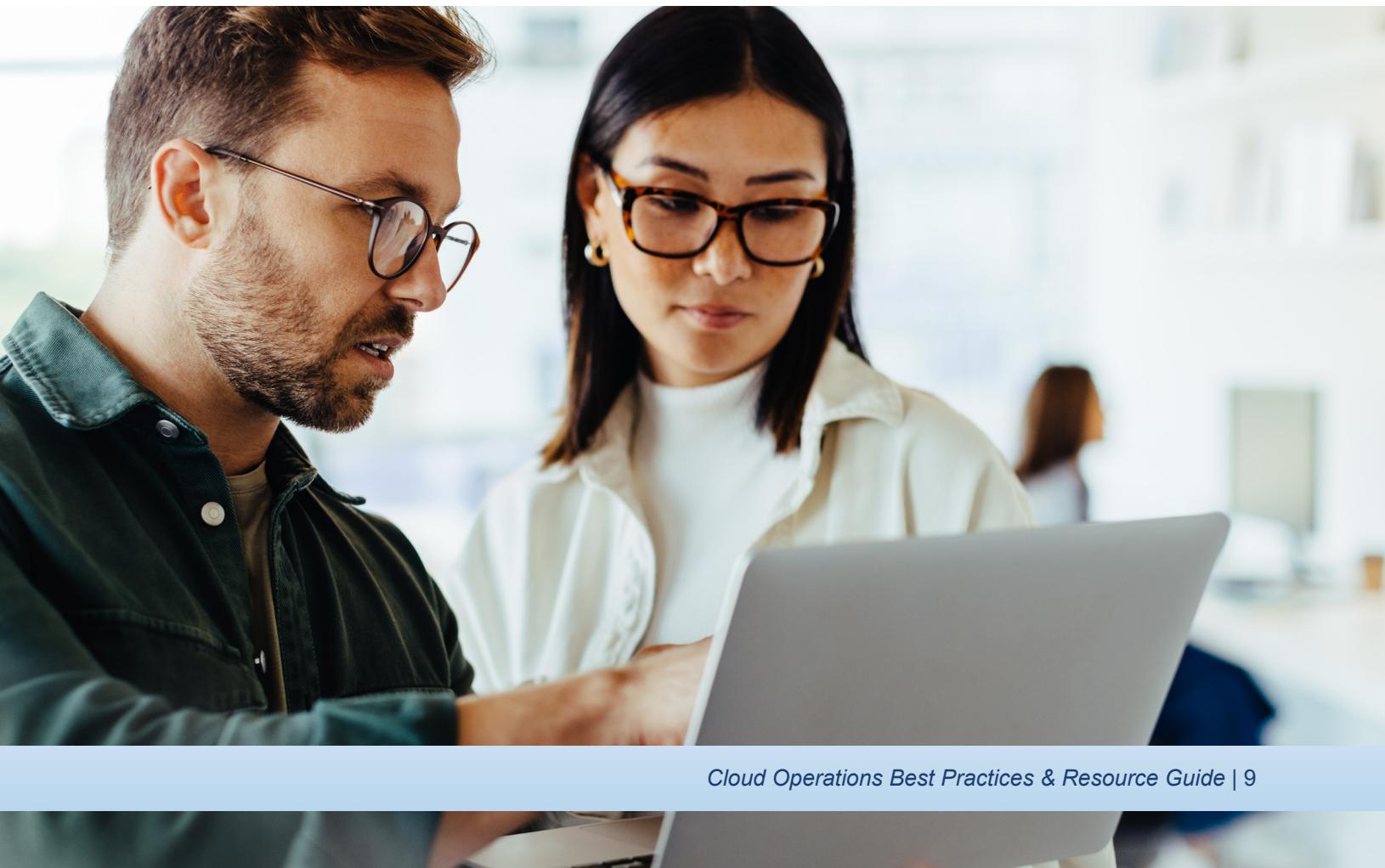


Figure 1: Important Knowledge Domains for Cloud Operations



CLOUD OPERATIONS VERSUS TRADITIONAL IT OPERATIONS

There are important differences between traditional IT and cloud operations. These differences can significantly impact decisions on how efficient and effective your cloud investments are purchased and supported. Table 1 summarizes some of the key differences between cloud and traditional IT operations.

Table 1: Key Operational Differences between Cloud and On-Premise Operations

Operations Categories	Cloud	On-Premise/Data Center
Infrastructure	Based on virtualized infrastructure, physical infrastructure is managed by the cloud provider.	Based on physical infrastructure, managed in-house.
Scalability	Designed for scalability, agencies can quickly and easily add or remove resources as needed.	Requires significant planning and lead time to scale up or down.
Cost	Costs can vary as providers charge on a pay-as-you-go basis and allow agencies to only pay for the resources they use. Significant data requirements constitute a thorough comparison between on-prem and cloud.	Typically requires significant capital investment upfront and fixed costs to support ongoing maintenance.
Security	Cloud providers are responsible for many aspects of cloud security.	Agencies are responsible for securing the physical infrastructure and implementing appropriate security measures.
Monitoring	Cloud providers can offer tools to monitor and manage an agency's cloud resources.	Agencies need to implement their own monitoring tools and processes.
Availability	Cloud providers can offer high levels of availability and uptime which are often backed by service level agreements.	Agencies need to implement redundancy and failover mechanisms to ensure high levels of availability.
Disaster Recovery	Cloud providers can offer robust disaster recovery options, such as backup and recovery services, to help agencies recover from catastrophic events.	Operators need to implement their own disaster recovery plans and solutions.

Operations Categories	Cloud	On-Premise/Data Center
Maintenance	Cloud providers are responsible for maintaining the cloud infrastructure, including performing upgrades and patching vulnerabilities.	Agency is responsible for maintaining its own IT infrastructure, which may require significant time and resources.
Automation	Rely heavily on automation tools and processes, such as infrastructure as code (IaC) and continuous integration/continuous delivery (CI/CD) pipelines.	May not be as automated and manual processes may be required.
Resource Utilization	As resources can be dynamically allocated and de-allocated as needed, agencies can have more efficient resource utilization.	With dedicated hardware for each workload, agencies may have lower resource utilization.
Geographic Location	Cloud providers can run workloads in data centers located in different regions to support higher availability and recovery options.	Agencies are limited to the physical location of the data center or on-premise facility.
Talent & Skills	Cloud operations require a different skill set than data center operations, including cloud technologies, automation, and DevOps tools.	Agency operations require more traditional IT skills like hardware and network management.
Infrastructure as Code (IaC)	Agencies can provision virtual resources using configuration scripts. This supports version control and can be tested like any other software.	Agencies will rely more on the manual management of infrastructure.
DevOps	Practices encourage collaboration between development and operations teams, enabling faster development and deployment of applications.	May involve more siloed teams and slower development cycles.
CI/CD	Code changes are deployed rapidly and reliably, often multiple times per day.	Require more time and effort to deploy code changes, which can slow development cycles

CLOUD-BASED RESOURCES CHANGE RESPONSIBILITIES

As agencies move from traditional IT operations to the cloud, their responsibilities change. With the cloud, agencies typically no longer manage basic services like power, connectivity, and physical security. Instead, the cloud service provider (CSP) manages all physical assets (e.g., servers, routers, firewalls and other components). With IaaS and to a lesser extent PaaS, the agency manages virtual resources including servers, firewalls, and other services.

But all cloud services are not equal. The types of responsibilities assumed by the agency will differ depending on the service provider and product. While there are many potential variations on this theme, the following offers some simplified scenarios for how the type of service will impact what an agency will need to do and what the vendor will do. Regardless of who does what, the agency is still responsible for conducting the appropriate due diligence to ensure a system is secure, well managed, and meeting expectations.

IaaS, PaaS, and SaaS

The three primary cloud prototypes are IaaS, PaaS, and SaaS.

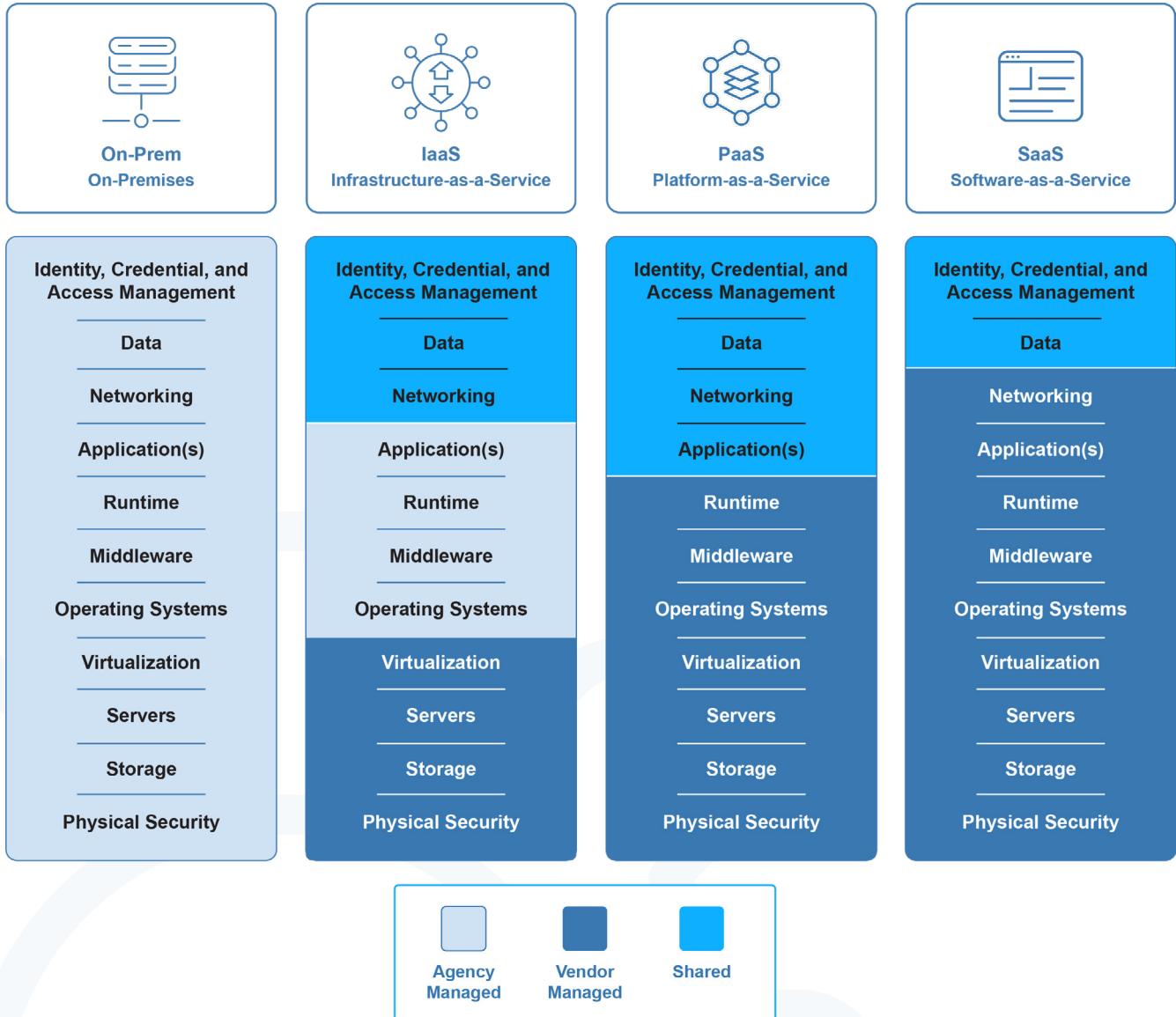
- IaaS is a set of virtualized computing resources that are highly configurable and are used to provide services over the internet.
- PaaS is a cloud platform used for developing and deploying applications without managing the infrastructure.
- SaaS is a cloud-based software application accessed over the internet.

As shown in Figure 2, responsibilities assumed by an agency change dramatically with the different prototypes. With an on-premise solution, a fully agency-owned and operated alternative, virtually all aspects of the environment are obligations assumed by the agency. With IaaS, these responsibilities are significantly reduced, as the provider manages all of the hardware, software and facilities. With PaaS, the responsibility for other key activities is transitioned to the provider. Finally, with SaaS, even more responsibilities are transitioned to the provider.

An important takeaway is that, while many responsibilities are changed, the agency is still responsible for the overall system security and function. Also, a number of important tasks will remain with the agency. These include:

- Managing costs and contracts
- Following required cybersecurity practices
- Managing user and role assignments
- Training users and support personnel

Figure 2: Changing Agency Responsibilities with On-Premise and Cloud Services





LEADERSHIP

As with any IT service, good leadership is essential to integrate your agency’s cloud assets with other IT offerings and provide the expected value. Strategy, high-level planning, an accurate view of the current environment, and organizational change management are key considerations for cloud operations leaders.

While leadership is often considered an “executive” function, this guide takes the view that the teams who read this guide will also be advising management on how to operate the cloud. At the highest level, the goals of the leadership function within cloud operations include:

- Ensuring that operations align with cloud strategy and planning
- Communicating the organizational vision and plans to all stakeholders
- Prioritizing resources to support cloud investments
- Continuously improving tasks and outcomes
- Assessing risks
- Investing in new features and technology

CLOUD OPERATIONS STRATEGY

Your agency’s cloud operations strategy should be part of the broader agency IT and Capital Planning Strategy. It should align to the agency’s business needs as well as current federal strategies and initiatives. Keep your strategy simple, and ensure it is well communicated to all relevant stakeholders. Finally, it should also reflect your program’s current realities, including program size and maturity. Refer to the [GSA Cloud Strategy Guide v1.1](#) for more information on developing a cloud strategy.





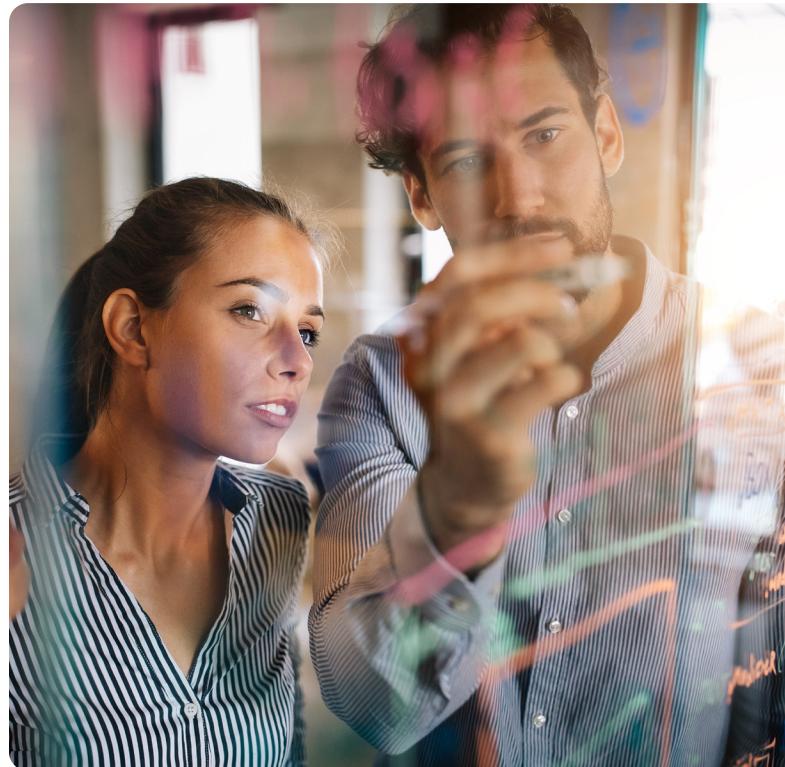
A cloud strategy will help guide your teams in developing the people, policies, and processes to best manage your agency's cloud assets. Cloud technologies are changing rapidly, so review the cloud strategy annually and update plans as needed to reflect emergent requirements and new technology or products. See the [Small Agency CIO and IT Executive Handbook](#) for many useful insights for agency leadership.

Below are potential considerations when developing a cloud operations strategy. They are not requirements but rather "touchpoints" that are strategic and impactful to operational concerns:

- Migrating existing assets to the cloud
- Building new capabilities or systems
- Establishing governance
- Addressing potential skills gap

PLANNING

A comprehensive multi-year, organizational plan for cloud investments lays the foundation for evolving agency cloud operations and preparing to meet upcoming demands. It should encompass IT and be developed in collaboration with your program offices and other key stakeholders. These plans should provide insights for program offices and cloud teams to map out and budget for their technology needs.



One approach is to develop a roadmap. This is a simple, high-level plan to give stakeholders context as to what functionalities are available and what new capabilities are planned. Ideally, the plan could be for two to three years, provide key assumptions, budgets, and outline strategic initiatives. Strategic initiatives might include the adoption of new frameworks such as DevSecOps, leveraging existing capabilities like elasticity, or implementing new tools including management platforms.

This type of planning will allow operations teams to think strategically as they implement tools and processes to manage and continuously improve agencies' cloud investments.

Multi-Cloud and Hybrid Cloud

The operational impact of multi-cloud and hybrid-cloud environments is an important topic for leadership since investing in multiple vendors or facilities can unexpectedly increase operational cost.

A multi-cloud or hybrid cloud involves using two or more CSPs, or an on-premise facility and one or more CSPs (See Figure 3). A multi-cloud and hybrid-cloud environment is common and



appropriate for many agencies. However, beware of the operational realities of managing across multiple CSPs, platforms, and services. Any new service, especially multiple IaaS providers, can complicate operations for the support teams. Each platform may have its own administrative tools, security needs, and training requirements. Moreover, they can present interoperability challenges since tools do not always natively integrate into your particular operational needs and will require some adaptation of processes or technologies. From an operational perspective, this can add costs to training, updating processes, and consolidating data. See the [GSA Multi-Cloud and Hybrid Cloud Guide](#) for more information.

The key takeaway is that providing a secure and reliable service that is within budget and meets expected quality can be *at risk* if the impact of operations is not properly assessed.

Advantages of Multi-Cloud and Hybrid Cloud

- Leveraging best-of-market innovations and capabilities
- Mitigating vendor lock-in by using two or more vendors
- Increasing agility, scalability, flexibility, and redundancy

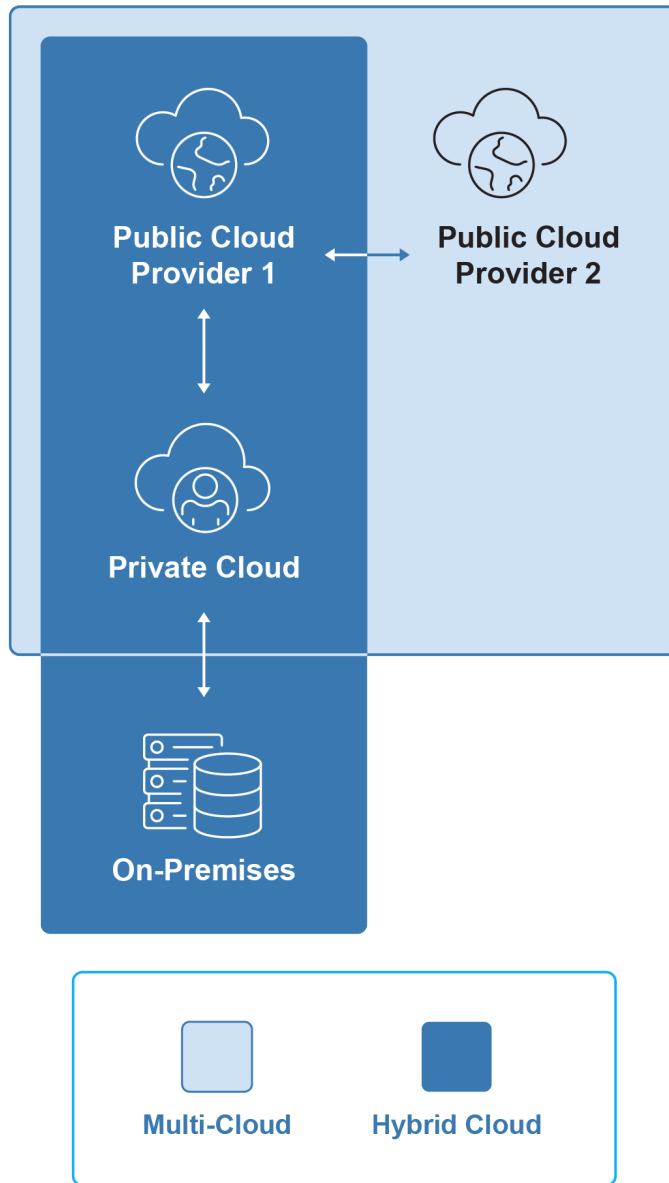
Disadvantages of Multi-Cloud and Hybrid Cloud

- Increased recruiting, hiring, and training costs
- Increasing management overhead
- Increased attack surfaces





Figure 3: Multi-Cloud and Hybrid Architecture



CURRENT STATE ASSESSMENT

Knowing where you are with respect to your cloud investment is crucial to defining the plan for the future. Consider the entire agency ecosystem that will implement, maintain, and use these cloud-based tools. See the Appendix I, [Assessing Readiness for Cloud Migrations](#), for a questionnaire used by a large agency to assess the ability of an office or program to migrate to the agency-managed cloud services. For a current state assessment, consider the following:



- **Evaluate people, processes, and technology.** Evaluate your agency's IT ecosystem by assessing people (functions, roles, skills), processes (frameworks, procedures, performance), and technology (tools, services, capabilities).
- **Review enterprise architecture.** Ensure you have up-to-date documentation for enterprise architecture and other processes.
- **Consider projects or initiatives.** Identify current, planned, and proposed projects or initiatives that may help or hinder cloud investments.
- **Evaluate prior assessments.** Review prior assessments like [Federal Information Technology Acquisition Reform Act](#) (FITARA) and [Federal Information Security Modernization Act](#) (FISMA) appraisals to identify challenges that could hinder or benefit moving to the cloud.
- **Assess applications for cloud migration.** Catalog and evaluate your applications to determine which applications should be migrated. *Note that some applications may not be good candidates for migration.* See [Application Rationalization](#) section.
- **Review existing IT governance.** Review all your IT governance policies and processes (e.g., configuration and change management) to identify gaps in your current approach relative to cloud offerings. *Note that the nature of the cloud will certainly benefit from agile decision making and execution.* See [Governance](#) section.
- **Assess your workforce.** Identify the necessary skills to effectively manage your cloud operations and analyze for possible gaps with respect to your current workforce. See [Workforce Planning](#).

Stakeholder Analysis

Successful cloud operations require both vertical and horizontal alignment within your agency. Identify relevant agency stakeholders and determine what their interests, goals, and expectations are relative to the performance and cost of your agency's cloud. See Table 2 for a sample of typical cloud stakeholders.

A stakeholder analysis will inform a comprehensive communications strategy and improve your collaboration. Conduct an initial stakeholder analysis as part of planning and reassess as your team and agency matures. See the [GSA Cloud Strategy Stakeholder Analysis](#) for more information.

Conducting a Stakeholder Analysis

1. Establish a purpose for this analysis, e.g., identify key stakeholders by interest and influence.
2. Identify stakeholders, including customers and vendors.
3. Segment your stakeholders, e.g., by role or by organization
4. Map your stakeholders against relevant categories based on your purpose, e.g., influence and interest.
5. Develop a plan or strategy to ensure stakeholder buy-in.

**Table 2: Sample Cloud Stakeholders**

Agency	Stakeholder
Agency IT	IT Operations
Agency IT	Plans and Programs
Agency IT	Enterprise Architecture
Agency IT	IT Security
Agency Supporting Offices	Procurement
Agency Supporting Offices	Finance/Budgeting
Agency Supporting Offices	Human Resources
Agency Supporting Offices	Application Business Owners
External to Agency	OMB
External to Agency	Congress
External to Agency	The Public/Press
External to Agency	Vendors

ORGANIZATIONAL CHANGE MANAGEMENT

Successful cloud operations require new tools, skills, and approaches. Agencywide adoption of technological innovation requires executive engagement, a plan, and team buy-in.

The cloud offers robust opportunities to manage resources and thereby costs. To fully leverage these benefits, an agency must change and adapt the way people work, the processes they follow, the tools they use, and the scope of their duties.

A solid Organizational Change Management (OCM) strategy can help agencies optimize cloud operations. OCM is a systematic approach to preparing, equipping, and supporting teams to embrace changes in processes, structures, or technologies. It involves planning, communicating, and implementing strategies to mitigate resistance, promote adoption, and drive successful outcomes during periods of organizational change. See Figure 4.



Typical goals for OCM include:

- **Strategy and Planning.** Agencies need to plan for change at the start of cloud adoption. They should identify and empower early adopters to advocate for change and the voice of the customer.
- **Messaging and Communication.** Agencies need to clearly articulate why adopting and maturing cloud operations is critical to both cost and value.
- **Business Integration.** Agencies should demonstrate the value of a change and its success at each level of the agency.
- **Process Improvement.** Agencies should highlight not only outcomes but also the innovations in processes and frameworks.

Figure 4: Organizational Change Management Approach





ORGANIZATIONAL DESIGN

When considering a new paradigm like cloud operations, an agency should also evaluate its organizing principles and organizational design. The current structure may reflect the agency's historical experience supporting traditional on-premise infrastructure. It may not be best suited to support and optimize a growing cloud infrastructure and may need updating.

New organizational designs may benefit from updated tools and processes that support strong communication practices. The more distributed organizational models will benefit from approaches that increase transparency and are actively maintained. These approaches include a community of practice, knowledge bases, and code repositories. A key outcome is to standardize enterprise practices that ensure development teams and business units have a common set of software engineering skills to avoid unnecessary technical debt.

A new organizational design should also be linked to a broader organizational strategy. The strategy and goals should appropriately align with the design. The following organizing principles should be considered when evaluating current and future states:

- **Governance:** Establish a governance structure with the necessary decision-making processes related to cloud operations, including change management.
- **Staffing:** Assess the skills and expertise of the existing IT workforce and identify any gaps that need to be addressed for cloud adoption.
- **Communications:** Foster collaboration between teams.
- **Security:** Address security policies and procedures.
- **Quality:** Implement quality management practices to improve processes, define targets and monitor performance.
- **Vendors:** Establish processes for vendor selection, contract negotiation, and ongoing vendor management to ensure service level agreements (SLAs) are met and risks are effectively managed. Consider how the contractor teams will be integrated into the federal teams for optimal performance.

Agencies will need to change minds to successfully transition to a new organizational design. The use of OCM strategies will be necessary to align your people, processes, and technology to create the greatest value. Examples of these challenges include:

- On-premise models were often managed through a centralized IT management structure and organization, which differs from new hybrid and multi-cloud environments.
- With cloud, more duties can be pushed out both geographically and organizationally, creating new business challenges and opportunities for teams.
- How well decentralization strategies work is in part a function of how well monitoring, automation, processes and policy are performed.



Selecting an Operating Model

Determining your agency's operating model will have significant impacts on downstream day-to-day activities like provisioning and deployments. Figure 5 provides an additional perspective on two opposing models.

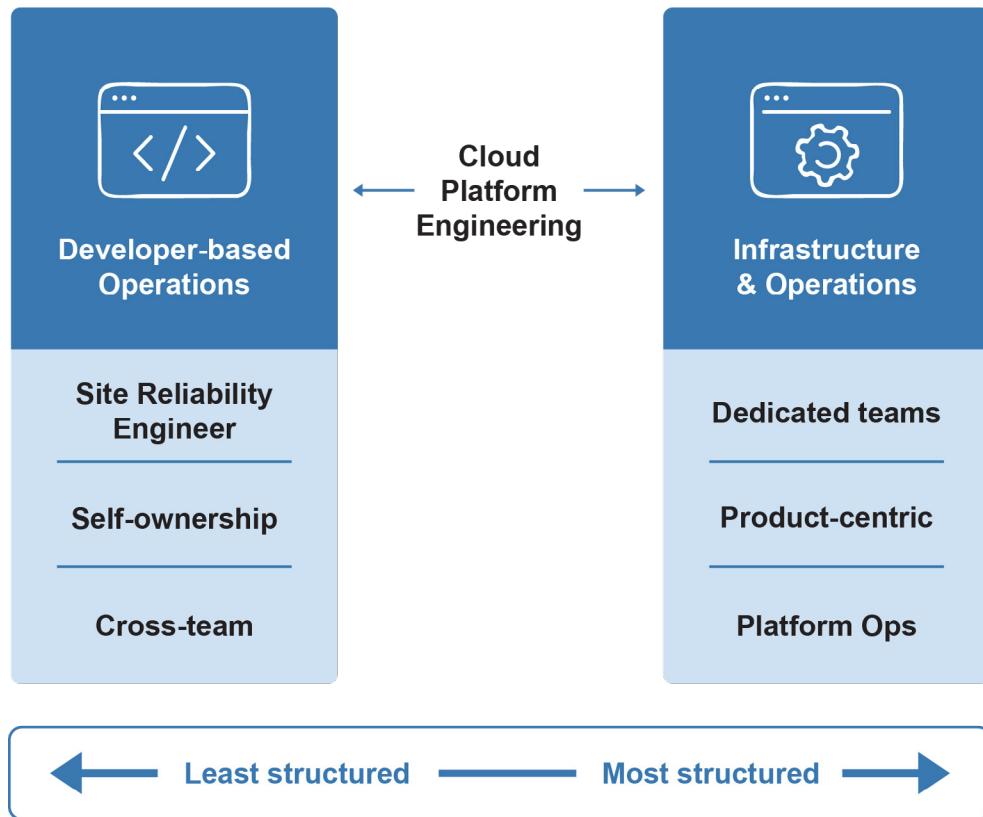
One strategy for identifying your agency's operating model is to identify preferred practices (e.g., provisioning) and then "back into" an operating model that supports the preferred practices. Agencies should consider the following issues when contemplating an operating model:

- Extent to which development is managed centrally or by offices
- How cloud operations are aligned to product, division, project, etc.
- Level of current and planned automation
- Extent that cloud services will be used for core operations (versus on-premise)
- Agency reliance on SaaS vs. IaaS and PaaS. There should be less focus on development issues and automation if there is a high reliance on SaaS products.





Figure 5: Paradigms for Managing Cloud Operations



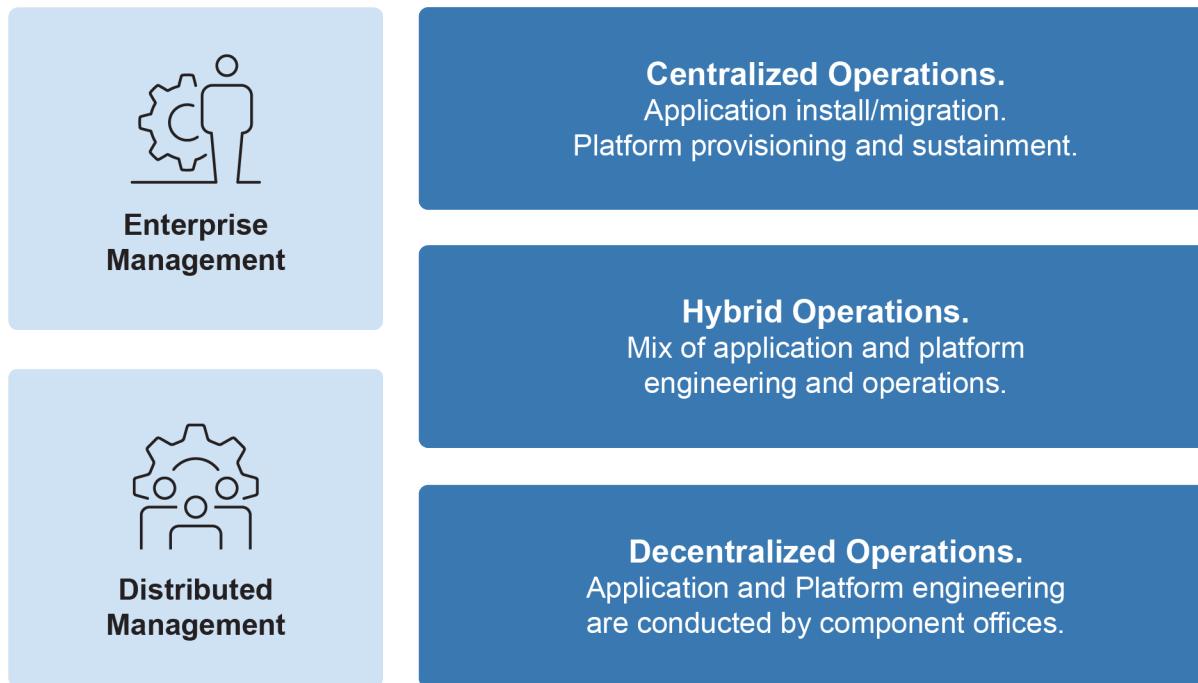
Organizational Designs to Consider

The organizational design to manage your cloud services should align with the agency's requirements, goals, resources, size, complexity, and other relevant measures. Be agile and prepared to evolve the chosen model based on new information, services, and products.

The three organization prototypes shown in Figure 6 below provide only a starting point for your agency. Many variations are possible. Whatever option you choose will need to be tailored to fit your organizational realities. Use these models to engage the stakeholders in a focused dialogue as you develop your own design.



Figure 6: Organizational Design Prototypes



Centralized. An enterprise team is responsible for managing all aspects of applications and platforms. This team includes experts in cloud technologies, infrastructure management, security, and compliance. They would typically handle provisioning, deployment, sustainment, and security. This structure supports standardization across the agency.

Hybrid. In this approach, an enterprise team is responsible for managing core infrastructure components, security, and governance. The enterprise team standardizes services, develops best practices, and provides support. The decentralized teams servicing the component offices have autonomy over certain aspects of the platform to support activities like provisioning and application deployment. This model attempts to find balance between standardization and flexibility.

Decentralized. Each component office has a dedicated team responsible for managing both application and platform. This allows for greater flexibility and customization, as teams can tailor the infrastructure to their unique requirements. Coordination and collaboration between teams become crucial to ensure consistency and alignment with overall agency objectives.



BUSINESS MANAGEMENT

Business management involves the backend operations required to maintain cloud environments. As your agency considers future changes or investments, be sure to address the basics including use case and return on investment. The following key areas are considered in this section:

- **Financial management** offers plans and controls cloud usage and spending.
- **Cost management** includes collecting, analyzing, and reporting cost information to more effectively budget, forecast, and monitor costs.
- **Performance management** implements cloud monitoring activities to optimize performance and meet performance goals.
- **Capacity management** considers data processing requirements over the whole service lifecycle and matches demand with available resources.
- **Quality management** defines and analyzes areas for improvement to deliver higher quality products and services.
- **Vendor management** oversees and controls relationships with cloud service providers and other third-party vendors.
- **Governance** guides the overall cloud operations environment with the appropriate policies and processes.
- **Portfolio management and rationalization** aligns an agency's collection of cloud resources to improve efficiency, reduce costs, and align with business objectives.
- **Workforce planning** supports the hiring, structure, and training of the cloud operations teams, including defining roles and responsibilities.

FINANCIAL MANAGEMENT

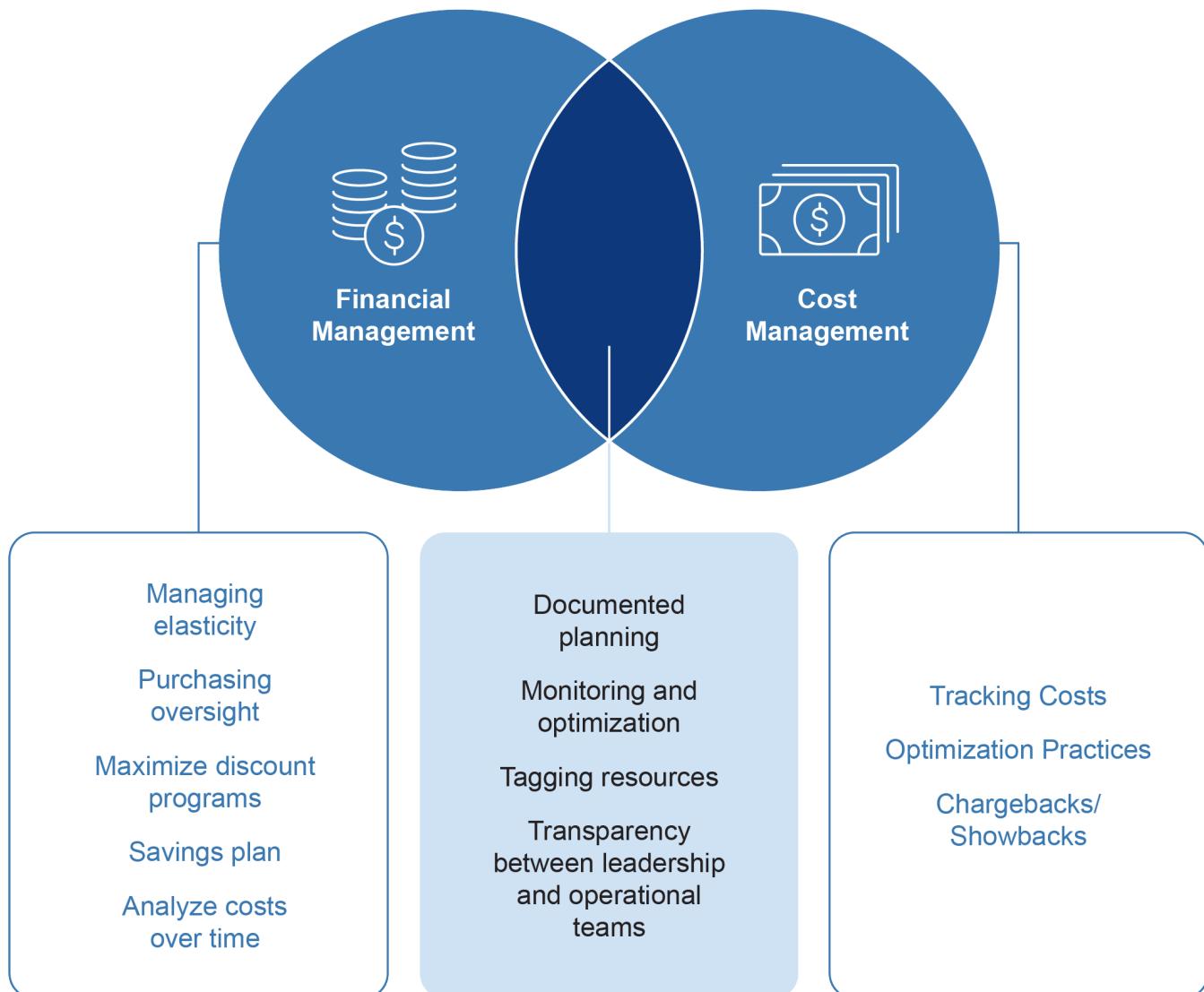
Effective financial management of cloud assets requires a structured approach to plan, budget and monitor your cloud investments. Both the strategy and tactics used to manage the cloud can significantly differ from those used for on-premise facilities or data centers. **In particular, the**



ability of the cloud environment to change quickly or dynamically may benefit from more agile funding approaches and more frequent budget reviews.

Establishing a structured approach to financial management will make activities such as forecasting and cost allocation easier to manage. Understanding the expected benefits of potential financial management tools can help outweigh their costs. See Figure 7 for key task areas within Financial and Cost Management.

Figure 7: Important Tasks by Financial Management & Cost Management Domains





Transparency between different functional teams such as finance and operations is imperative. Transparency is enabled through agency culture, well-understood processes, and shared data. Specific areas that may need immediate attention include:

Purchasing. With an on-premise model, purchase requests are part of a well-defined set of processes (e.g., request, approval, purchase, and implementation). With the cloud, it is possible and even desirable for frontline engineers to add new resources without any additional approvals. These resources usually correspond with additional costs and can drive up your agency's IT spend. Thus, the key is to ensure that sufficiently robust management controls are in place to identify and control new services and associated costs.

Elasticity. Cloud services often have the ability to add and subtract resources on demand, and cloud resources can be turned off when not in use. As these resources are typically associated with a pay-as-you-go model, identifying and managing these assets will have a direct impact on cost. Agencies should understand when elasticity is agency-controlled (e.g., IaaS) versus vendor-controlled (e.g., SaaS) to best optimize cost.





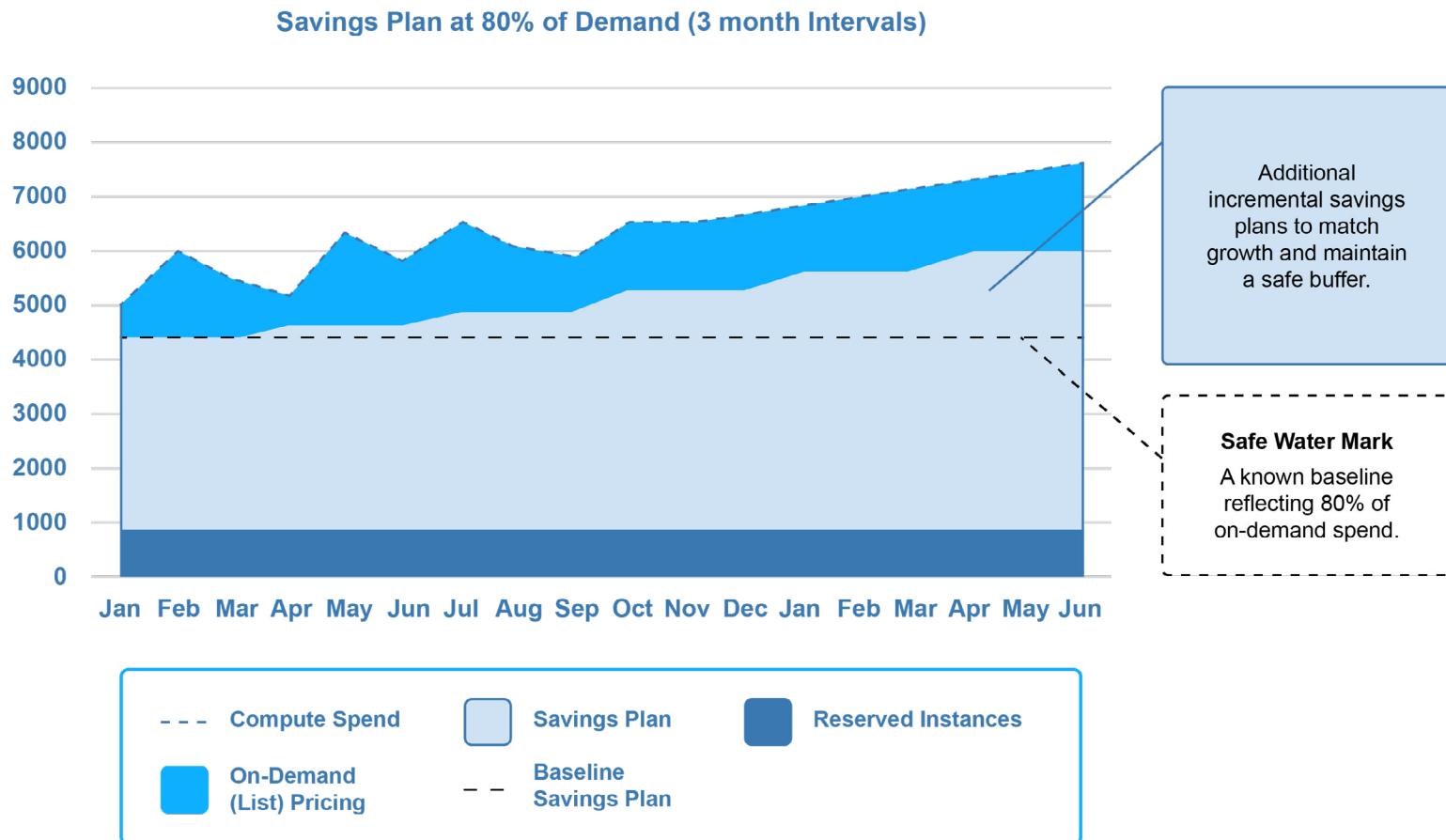
Similarly, **savings plans** provide agencies with a discount on their usage in exchange for a commitment to a consistent amount of usage, measured in dollars per hour, over a one- to three-year term. Unlike reserved instances, savings plans provide greater flexibility in terms of instance type, region, and operating system. This makes them suitable for customers with variable workloads or those who require flexibility in resource allocation.

Some additional tactics for reducing cloud costs are noted below and represented in Figure 6: Eighteen Month Purchasing Strategy Using Discount Programs.

- Minimize on-demand (list) pricing with the combination of reserved instances and savings plans.
- Choose a “safe watermark” around 80% of the consistent spend rate to account for unexpected declines in demand.
- Additional savings plans are purchased over time (quarterly in Figure 8) to match consistent increasing demand.



Figure 8: Eighteen Month Purchasing Strategy Using Discount Programs (Example)



Minimize On-Demand (list) pricing with the combination of Reserved Instances and Savings Plans.

Choosing a safe water mark around 80% of the consistent spend rate accounts for any unexpected decline in demand.

Additional Savings Plans are purchased over time (shown quarterly) to match consistent increasing demand.



Funding Considerations. Due to the [Anti-Deficiency Act](#), commitments like reserved instances and savings plans can only be paid in arrears. This can mean the potential discount is reduced. Note that some agencies will undertake one-year commitments with respect to these discount programs.

Be sure to work with your agency's finance and contracting offices to determine your funding obligation approach and gain prior approvals for timeframes and payment schedules.

COST MANAGEMENT

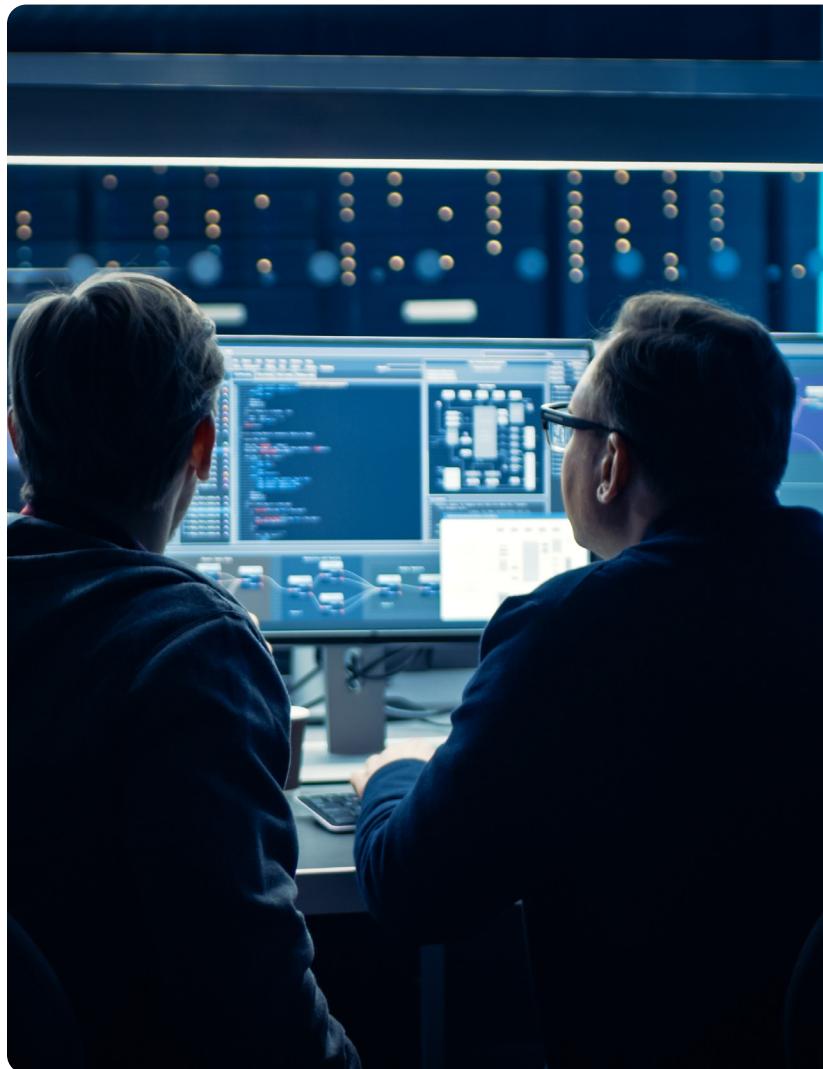
Cloud cost management is the practice of monitoring cloud resources to optimize cloud-related costs. Optimization identifies areas where cloud resources may be unused or idle for periods of time. Opportunities to optimize may include consolidating resources, removing unneeded resources, and exploring potential discount programs. Your goal is to continuously assess your cloud resources to identify opportunities to reduce costs.

Cost optimization uses actual usage data to inform decisions and reduce overall cloud costs. As such, a regular monitoring cadence is important. It is common for metrics to be calculated by week, day, or hour.

Monitoring is effectively “baked in” to the cloud environment and far surpasses the monitoring data typically available from on-premise settings. The available data from these environments is also granular with respect to both resources and time. Understanding how to analyze this data is critical and requires insight into both the technical environment and analytic tools. Without effective monitoring and analysis, an agency will not be able to optimize costs.

Strategies like tagging cloud resources and account management should be used to classify resources for monitoring, optimization, chargebacks, and showbacks. Additionally, analytics will provide far more insight if the analysis looks beyond simple monthly cloud spend and assesses by week, day, and possibly hour.

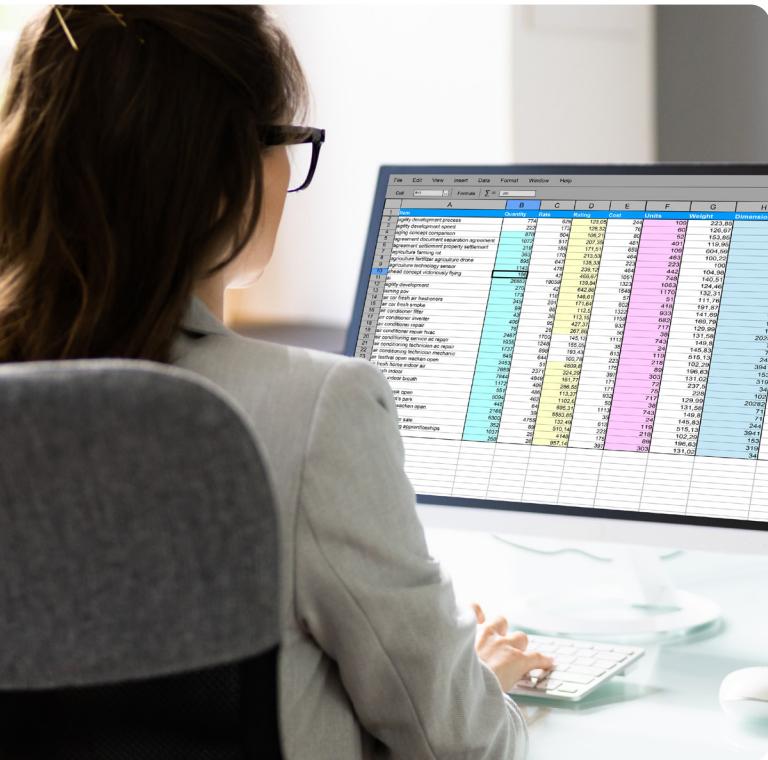
The CIO Council's [Federal Technology Investment Management \(FTIM\) Community of Practice](#) has been conducting extensive research, education, and pilot programs





using methodologies that support a disciplined approach to financial and cost management for IT resources used by federal agencies. These include [Technology Business Management](#) and [FinOps](#).

The following sections offer specific practices to manage costs.



Tracking Costs

A good methodology for tracking expenses is a critical step towards optimizing costs and supporting chargebacks. A recommended approach, shown below, is to use both account management and resource tagging strategies to support the necessary analysis.

- Using the account management structure aligns costs to funding, business units, and dev-test-prod environments. However, cost data at the account level is typically at a high level and lacks detail.
- Using resource tagging allows you to:
 - Compile costs at a system, service or application level.
 - Build a cost model of an application or service.
 - Understand the cost drivers and optimization opportunities.

Cloud Account Management

The implementation of a multi-account architecture within a given IaaS environment provides a number of benefits, including well-defined security boundaries, efficient cost management, and resource isolation. Work with your IaaS vendor to understand their particular implementation of account management, as this will vary among vendors. See Figure 9: Typical Account Management Structure.

By using separate accounts for different workloads or applications, you can isolate resources. This allows application developers or other users with high-level permissions to be given the access required to manage their resources without impacting resources outside of their areas of responsibility. This may include self-service provisioning and control of resource or application specific security groups. Using accounts as a cost boundary allows for a more automated and straightforward way of tracking costs for individual projects, departments, or business units than tagging alone. Using separate accounts for testing and development helps ensure changes do not impact production workloads. This provides a controlled and isolated environment for developers while reducing the risk of disrupting critical systems.



Leadership



Management

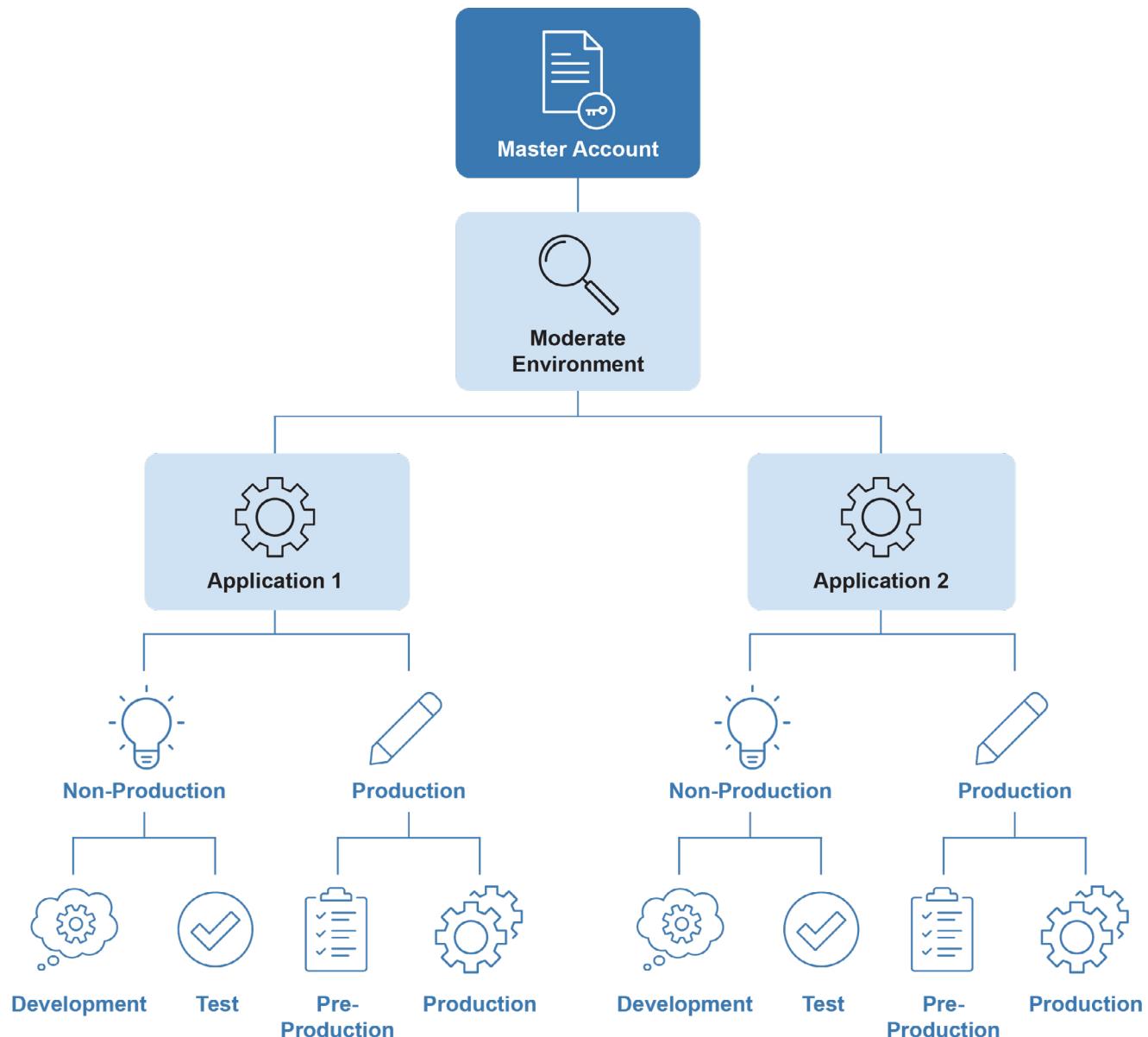


Security



Engineering

Figure 9: Typical Account Management Structure





Resource Tagging

Resource tagging provides a flexible and customizable way to effectively manage cloud resources. It enhances visibility and streamlines operations by supporting resource management, cost allocations, policy enforcement, automation, security, and reporting. With an effective tagging strategy, an agency increases its ability to optimize all aspects of cloud operations.

Developing a Cloud Tagging Strategy

The GSA [Cloud Tagging Strategy Guide](#) offers the following five-step process to help agencies create a cloud tagging strategy:

1. Customize tags according to users' needs and technical, business, automation, and security goals.
2. Identify and categorize stakeholders based on their interest and influence.
3. Determine functional tagging requirements and prioritize the needs of the most influential and interested stakeholders.
4. Using cloud design documents from CSPs, naming and tagging conventions, and governance, define tags and standardize their adoption.
5. Implement tags across the agency using nomenclature templates and governance documents, and set an enforcement deadline.

The following should also be considered while developing a cloud tagging strategy:

- Tagging parameters vary by CSP. If you are working in a multi-cloud or hybrid environment, you need to consider your tagging requirements in the context of these different providers.
- Tags are case sensitive, so even slight variations in the tag used for each service can result in some usage not being associated or attributed correctly.
- Use automation to tag resources and minimize human error.
- Tagging also helps in establishing dependencies so you can link resources to one another (e.g., compute to storage). With these associations, you can ensure all services within the IaaS ecosystem are properly decommissioned (e.g., deleted or archived).
- There needs to be a strong tagging policy that addresses nomenclature and accountability to ensure high conformance.
- While not all resources are taggable, they still incur costs and are necessary. You can roll up these costs to the account/subscription level.



Optimization Practices

Monitor Rehosted Applications

When planning for rehosted type (e.g., lift-and-shift) migrations, your migration team may target lower compute utilization rates than those required for cloud-native solutions. For example, the migration team may re-host an application with a target compute utilization of 70%, whereas a cloud-native application might target 90% utilization.

This additional, and possibly unused, capacity needs to be reflected in the analysis of performance, forecasts for future needs, and finally as a datapoint for potential cost savings for relevant initiatives.

Budget Alerts

Create monitoring policies and alerts for actual spend. This approach is especially important if your cloud operations are decentralized. Use alerts to set thresholds across the desired timeframe (e.g., daily, weekly, monthly, quarterly). For greater oversight, alerts can be created for planned surge timeframes. Approval workflows can be created if the planned spend needs modifications or an increase.

Scheduling

Scheduling provides the ability to turn off services when they are not in use and turn them back on when they are needed again. Most CSPs have configurable scheduling features that can automatically start and stop services (e.g., virtual machines [VMs], database) based on the relevant business needs. A common use case is development and testing servers that are not typically required to run 24/7 and, therefore, can be turned off by schedule. See Figure 10 for a simple example of potential cost savings for systems that only need to operate during business hours.

Figure 10: Potential Savings for Cloud-Based Service Running Only During Business Hours





Snapshots

Snapshots are a mechanism for creating a backup of a system's current state. New snapshots typically do not overwrite older ones. A policy should be put in place that determines the best fit for the snapshot lifecycle, such as archived or deleted. Snapshots should be managed on a daily or weekly basis so older snapshots are deleted. In many cases, this process can be scripted and automated. Note that "snapshots" are distinct from "backups" in purpose and features.

Disk Volume Storage Rightsizing & Unattached Storage

Disk volume storage is often over-provisioned or underutilized. Storage units can also become orphaned or 'unattached' after an instance is stopped or decommissioned.

Disk volumes should be right-sized to the need. When considering storage, distinguish between IOPS and throughput as they both have cost implications. Input/Output Operations Per Second (IOPS) is the count of disk operations per second, and throughput is the volume of data being transferred per second. Your cloud provider will have tools (typically a command-line interface [CLI] or a dashboard) that can be used to identify these underutilized or unattached resources.

For unused storage, identify the proper disposition for the resident data. One option is archiving items to lower cost storage and deletion.

Be sure to follow the agency's records retention guidance. Consult your Senior Agency Official for Records Management or other appropriate agency contact. The [National Archives' Federal Records Management](#) site provides many useful resources as well.

Logging Management

Log management is a continuous process of centrally collecting and analyzing system-generated data to provide actionable insights to support troubleshooting, performance, and security. This process can generate hundreds of gigabytes of log data per day. A log management strategy needs to analyze logs, report on them, and delete the log data once it is no longer needed to avoid wasteful data storage costs.

Federal log management falls under memo [M21-31](#), which details what has to be logged. There are requirements for log retention for each category of logging, typically 12 months of active storage followed by 18 months of cold storage. Maintaining large amounts of logs can have a significant cost and agencies should estimate costs to the greatest extent possible. Additionally, some logs constitute an official record and must be retained according to agency records retention policies. Consult with your agency records manager to get a clear understanding of retention requirements.



Compute Rightsizing

There is not a one-to-one relationship between on-premise resources (Central Processing Unit [CPU], memory) and cloud resources. Often, an on-premise system has a one-to-one relationship between systems and servers. However, in cloud environments, you can have a one-to-many type relationship with respect to resources and applications. With this relationship in mind, it becomes obvious how overprovisioning and underutilization are common pitfalls when moving systems from on-premise to the cloud using a lift-and-shift migration.

With due diligence, agencies can right-size their compute resources. CSPs have many different compute resources that vary in capacity and cost. For example, by monitoring and analyzing your services, an agency could move to a lower cost cloud resource.

Analyze at least one month of data (preferably more) to capture average and peak workloads. Adjust resources to better align with the established workload. Perform a monthly review to further refine your environment. Note that some cloud-native tools can perform assessments and provide recommendations for right-sizing your environment. See Table 3 below for an example of how costs may be allocated for different compute resources. In this example, by rightsizing the total hourly cost, a \$5.95/hour savings is realized. This is a substantial savings when realized over weeks, months and years.



Table 3: Sample Cost Savings by Changing Instances to Lower Cost Resources

Instance Number	Instance Type Before Rightsizing	Hourly Cost Before Rightsizing	Instance Type After Rightsizing	Hourly Cost After Rightsizing
VM1	Standard_DS2_v2, 2 vCPUs, 7 GB RAM	\$0.10	Standard_B2s, 2 vCPUs, 4 GB RAM	\$0.04
VM2	Standard_DS3_v2, 4 vCPUs, 14 GB RAM	\$0.20	Standard_B2s, 2 vCPUs, 4 GB RAM	\$0.04
VM3	Standard_DS3_v2, 4 vCPUs, 14 GB RAM	\$0.20	Standard_B2s, 2 vCPUs, 4 GB RAM	\$0.04
VM4	Standard_DS4_v2, 8 vCPUs, 28 GB RAM	\$0.40	Standard_B2s, 2 vCPUs, 4 GB RAM	\$0.04
VM5	Standard_DS4_v2, 8 vCPUs, 28 GB RAM	\$0.40	Standard_B2s, 2 vCPUs, 4 GB RAM	\$0.04
VM6	Standard_DS5_v2, 16 vCPUs, 56 GB RAM	\$0.80	Standard_D2s_v3, 2 vCPUs, 8 GB RAM	\$0.05
VM7	Standard_DS5_v2, 16 vCPUs, 56 GB RAM	\$0.80	Standard_D2s_v3, 2 vCPUs, 8 GB RAM	\$0.05
VM8	Standard_DS11_v2, 16 vCPUs, 56 GB RAM	\$1.00	Standard_D2s_v3, 2 vCPUs, 8 GB RAM	\$0.05
VM9	Standard_DS11_v2, 16 vCPUs, 56 GB RAM	\$1.00	Standard_D2s_v3, 2 vCPUs, 8 GB RAM	\$0.05
VM10	Standard_DS12_v2, 32 vCPUs, 112 GB RAM	\$1.50	Standard_D2s_v3, 2 vCPUs, 8 GB RAM	\$0.05

Total Hourly Cost Before Rightsizing - \$6.40**Total Hourly Cost After Rightsizing - \$0.45**



Chargebacks and Showbacks

Whether assumed or shared, an agency should be able to quantify the agency's cloud investment, demonstrate its value, and allocate costs. Then, an agency should provide this data to its stakeholders to establish a shared understanding about the agency's cloud investment decisions.

Calculating chargebacks and showbacks is a method for distributing cloud costs and demonstrating value. For chargebacks, a formula is used to allocate the costs to the appropriate groups. For showbacks, a formula is used to demonstrate the value rather than request payment.

Both chargebacks and showbacks require an allocation strategy. This strategy will benefit from a well-considered approach to use [cloud accounts](#) and [resource tagging](#). A cloud account is a hierarchical accounting model used for billing. Resource tags allow cost aggregation by resource. These approaches should be combined.

The allocation method should be easy to understand and fully leverage the available data. Three typical allocation strategies are:

- Even Split: Divide cost by number of clients
- Proportional: Direct to client cloud cost; count or size of resources
- Actual: Tracking consumption data to the client, system, or service

PERFORMANCE MANAGEMENT

Performance management analyzes and presents data to evaluate performance and return on investment for cloud operations. Establishing metrics is specific to the reporting needs of the agency. Determining the specific set of metrics to track cloud performance varies by agency and depends on mission, goals, services, and size. Select your metrics based on the desired analysis.

Monitoring tools provide insight into the performance and the availability of cloud services. The data collected as part of cloud monitoring can help determine which areas are more susceptible to potential outages or failures. The analysis of performance monitoring data should inform decisions on what to upgrade, add, or optimize.

Be thoughtful in how you manage performance monitoring.

Balance the need for performance monitoring with potential impacts on the system itself.

Also, be careful in collecting data that cannot be analyzed or is collected without purpose. See the [List of Common FinOps KPIs](#).



CAPACITY MANAGEMENT

Capacity management ensures an agency's IT resources can handle data processing requirements over the whole service lifecycle. Capacity planning matches demand with available resources and also forecasts expected trends. The main objectives of capacity management include:

- Determine the capacity needed to handle the present and future workloads.
- Develop and maintain a capacity management plan.
- Make sure performance objectives are completed on schedule and on a budget.
- Monitor capacity continuously to assist the [service management](#).
- Assist in diagnosing and resolving operations incidents (see [Service Resolution](#)).
- Analyze the impact of deviations on capacity and take proactive measures to improve performance where it is most cost-effective.

Capacity management ensures systems are functioning and meeting objectives without over provisioning resources. The agency can cut expenses and boost productivity by identifying and removing unnecessary resources (see [Typical Optimization Practices](#)). With proper monitoring, bottlenecks and equipment breakdowns can be anticipated and prevented.

Capacity management tools and methodologies should provide insights on resources and operations. Agencies should use these tools to monitor the volume and speeds at which an agency's applications move data through the IT infrastructure. The software and hardware elements that should be monitored include cloud services, end-user devices, networks and related communications devices, servers, and storage systems, and storage network devices. See [Appendix 2: Capacity Planning Template](#).

Current systems should be assessed for initial resource allocations and utilization by collecting and analyzing capacity data on a regular basis in order to gauge their performance and forecast demands. Some proactive capacity management and planning activities include:

- Monitoring network, compute, and storage capacity
- Analyzing and forecasting network, compute, and storage capacity
- Building models based on planned updates
- Efficiently executing changes to capacity
- Planning and optimizing performance and efficiency

One potential outcome of the capacity management process could be the movement of data from higher cost storage to lower cost storage. Decisions on data cleanup should consider business requirements and agency data retention policy



QUALITY MANAGEMENT

Quality management should be integrated into cloud operations and be applied across the entire system's lifecycle. Leadership, cloud operations, and other stakeholders should align on expectations for quality. Quality measures should be used for administrative processes as well as technical performance. This is especially important given the possibility for more frequent changes in a cloud platform.

Qualitative differences between cloud-based and on-premise environments in the context of quality management include:

- **Responsibility.** Cloud environments change the responsibility structure relative to on-premise environments. See Figure 2 on changing responsibilities. While an agency needs to ensure all aspects of its computing environment are conforming with expectations, the approach will differ for the cloud. For example, an agency will be more dependent on service level agreements to ensure conformance to certain performance standards.
- **Dynamic Resources.** It is much easier to turn resources on and off, as well as deploy new resources. While this capacity for change is critical to meeting changing demand requirements, it also introduces many more opportunities to create variations that can negatively impact security, performance, and cost.
- **Contracted Services.** Managing your environment must include service level agreements with the appropriate vendor. Ensure these agreements align with your agency's needs and that the vendor is meeting these standards.





Quality Principles

Quality management is a collection of tools and frameworks an agency uses to maintain and improve the value of its output. A good starting point is the ISO 9001 Standards. See Figure 11 below.

Figure 11: ISO 9001 Quality Management Principles





The seven quality management principles are:

- **Customer Focus.** Maintain trust with the customer through high quality products that meet their requirements and expectations. Sample measures include customer satisfaction, reliability, and performance.
- **Leadership.** Quality is top of mind at all levels of an agency. Leadership supports with word and deed in maintaining high performing environments.
- **Engagement.** Identify all your stakeholders and address their needs. This is an evolving area that needs to be refreshed to capture current state issues and attitudes.
- **Process Approach.** Use processes to support quality. Focus on evolving replicable processes that can reliably produce results.
- **Continuous Improvement.** Grow a continuous improvement mindset. Leverage [OCM](#) practices.
- **Evidence-Based Decision Making.** Use data to support decision making. Whether utilization statistics for resources or opinions from stakeholders, use available data to make choices and test hypotheses.
- **Relationship Management.** Engage stakeholders to keep them properly informed. Use these engagements to track opinions and expectations.

Example Use Case

Context:

A federal agency with a substantial cloud infrastructure that enables key mission goals and objectives.

Goal:

Ensure that cloud operations run efficiently and effectively, meet performance and availability targets, and deliver a high quality experience to customers.

Principles in Practice:

Infrastructure Monitoring. Continuous performance monitoring includes the availability of virtual machines, databases, storage systems, network connectivity, and other critical components. Alerts should be set up to notify the operations team when deviations from expected performance metrics occur.

Incident Management and Resolution. Leverage quality management principles to ensure incidents are properly documented and analyzed for root causes, corrective actions taken, and preventative steps established.

Test Execution and Automation. Automate testing processes and gather metrics to identify bottlenecks. Run testing in parallel platforms to reduce testing time and improve overall test coverage.



Scalability and Performance Testing. Scale up or down the resources needed for performance testing to accommodate changes in workload.

Performance Optimization. Capture data on cloud performance monitoring tools to identify bottlenecks, optimize resource allocation, and fine-tune configurations to pursue optimal performance.

VENDOR MANAGEMENT

Vendor Management develops and maintains effective partnerships with vendors. It involves the identification, evaluation, selection, and monitoring to ensure vendors meet your agency's requirements. Review the following when considering vendor management:

- Reach out to the GSA IT Vendor Management Office (ITVMO) via the web or the ITVMO mail. The ITVMO serves as a trusted independent advisor and advocate to help agencies buy common IT goods and services in compliance with procurement laws. The ITVMO's service offerings include Original Equipment Manufacturer (OEM) assessments and contract reviews. The ITVMO has also developed in-depth acquisition guidance, including PDFs and videos, for several vendors. See [Original Equipment Manufacturers \(OEM\) Assessment Initiative](#).
- Use the GSA Market Research As a Service to conduct effective market research as part of your acquisition planning stages.
- Carefully evaluate your value-added resellers (VARs) and other vendors providing development or operational support. Evaluate their ability to provide and maintain resilient systems that meet service-level objectives (SLOs) for availability and performance. Depending on your needs, evaluation criteria might include:
 - Providing expertise with appropriate certification
 - Providing Infrastructure as Code (IaC) to automate provisioning and deployments
 - Ensuring autoscaling and other cost-aware practices are used
 - Integrating systems into existing monitoring tools
 - Using automation to handle application issues
- Monitor consumption and avoid overspending with customized reports. Request that your vendor provides reports with customized views to support:
 - Internal chargeback and showback requirements
 - Trending by category of service or internal customer
 - Ingesting usage and billing reports into reporting tools
- Request customized invoicing to support:
 - Monthly vs. quarterly billing to better track consumption
 - Combining multiple payer accounts into a single invoice



- Combining usage and utility with professional services, training, and marketplace
- Separating invoices by customer-defined billing codes or programs
- Understand how your current software license requirements may be impacted by the CSP you select. Some software original equipment manufacturers (OEMs) will place restrictions on which clouds are “compatible” with their licenses. Depending on this compatibility, you may be required to purchase additional licenses.
- If you are developing a multi-year contract, negotiate for concessions such as service credits or discounted pricing to offset the initial migration costs.
- It is vital to work with the Contracting Officer and Contracting Officer Representative to determine your agency’s approach to billing. In particular, have discussions about advance payments. Advance payments are associated with reserved instances and annual SaaS subscriptions.
- Focus on performance-based solutions, SLAs, and terms and conditions that prioritize workloads and outcomes, as opposed to traditional “prescriptive” procurement requirements that specify what components the underlying infrastructure stack should contain.

GOVERNANCE

“Through 2025, more than 99 percent of cloud breaches will have a root cause of a customer misconfiguration or mistake.” [Gartner]

Cloud governance is the framework of policies that manage cloud operations within an agency. The governance process manages how cloud services are used, facilitates consistent performance, and supports the important goal of continuous improvement.

Cloud governance policies help ensure that all aspects of cloud operations are working towards the strategic goals of the agency. An effective governance model can reduce so-called ‘shadow IT’ where systems are deployed without the knowledge of the cloud services team. See Table 4: Cloud-Relevant Policies for Agencies to Consider.

Table 4: Cloud-Relevant Policies for Agencies to Consider

Policy	Scope of Policy
Resource Allocation	Define guidelines for allocating resources, such as virtual machines (VMs), storage, and networking components. Specify the process and criteria for provisioning resources based on workload requirements, performance considerations, and business needs.
Resource Monitoring	Establish policies for monitoring resource utilization within the IaaS environment. Determine the frequency of monitoring, metrics to be tracked (e.g., CPU usage, memory utilization, network bandwidth), and thresholds for triggering alerts or scaling actions.



Resource Sizing	Establish guidelines for right-sizing resources to optimize performance and cost. Determine the appropriate size (e.g., CPU, memory, storage capacity) for different types of workloads to ensure efficient resource utilization without overprovisioning.
Availability and Redundancy	Specify requirements for ensuring high availability and redundancy of resources. Define policies for deploying resources across multiple availability zones or regions to minimize the risk of single points of failure.
Resource Reservation	Define guidelines for reserving resources to guarantee availability for critical workloads. Establish criteria for identifying workloads that require reserved instances and specify the process for reserving and managing such resources.
Resource Decommissioning	Determine procedures for decommissioning unused or underutilized resources. Define guidelines for identifying and reviewing inactive resources and specifying the actions to be taken, such as resource termination, archiving, or repurposing.
Backup and Recovery	Establish policies for data backup and recovery within the IaaS environment. Determine backup frequencies, retention periods, and procedures for data restoration. Specify backup storage locations and encryption requirements.
Resource Tagging and Categorization	Define policies for tagging and categorizing resources to enable better resource management and cost allocation. Establish naming conventions, metadata attributes, and tagging requirements to facilitate resource tracking, reporting, and accountability.
Resource Ownership and Access Control	Specify guidelines for resource ownership and access controls. Determine the roles and responsibilities of resource owners. Define processes for granting and revoking access permissions. Enforce least privilege principles to restrict access to resources.
Resource Lifecycle Management	Establish policies for managing the lifecycle of resources. Determine procedures for resource provisioning, usage tracking, regular review of resource utilization, and retirement or decommissioning of resources no longer needed.
Resource Cost Management	Define guidelines for managing resource costs within the IaaS environment. Establish practices for monitoring and optimizing resource usage to minimize unnecessary expenses. Specify guidelines for analyzing cost reports, setting budgets, and implementing cost-saving measures.
Provisioning & Deployment	Define guidelines and standards associated with provisioning (setting up and configuring the underlying infrastructure) and deployments (deploying applications or services onto the provisioned infrastructure). Includes associated governance and catalog updates..
Configuration Management	Define guidelines and governance associated with managing resource information and metadata with respect to any change in the associated environment.



Governance should be right-sized based on the agency's risk tolerance, culture, size, and level of centralization. Policies should be re-assessed as part of a regular cadence and also as needed. Regardless of what policies are defined, this should be a careful and deliberate process that is well-communicated with all stakeholders.

Cloud operations governance should employ automated guardrails where possible. Automated guardrails are predefined rules, policies, or mechanisms that enforce selected governance and security measures. These guardrails help ensure compliance, mitigate risks, and maintain operational efficiency. Automated guardrails typically leverage cloud management platforms or infrastructure-as-code tools to enforce and maintain consistent configurations across the cloud resources. Examples include: [tagging](#), access control, environment creation, and capacity constraints. All automation should be documented as part of a comprehensive and widely accessible service catalog.

Use policies and procedures where automation cannot be used. Some of this guidance may need to be updated to reflect the new realities of the cloud such as change and configuration management, while others may be particular to the cloud such as resource tagging.

These technical controls can either be preventative or retrospective. Prevention is always the preferred approach.

- **Preventative.** Native controls within a cloud environment that prevent certain actions. For example, these could include:
 - Role-based access controls that prevent unauthorized resource access
 - Allow and disallow options based on geographic location for access
 - Specific network protocol enforcement
 - VMs deployments limits based on certain criteria such as certain memory or CPU configurations
- **Retrospective.** An inspection process to identify an issue or policy violation after the fact.

Developing Policies

The following provides three recommendations for updating or initiating a cloud governance process.

1. Establish an intra-agency governance team. This team can be an independent team or part of an established center of excellence or similar group of cloud experts designated to provide support and guidance on cloud-related issues.
2. Create agency governance principles. These principles will drive implementation as technical controls or organizational policies. Sample principles include:
 - a. Security as the foundation of the governance model.
 - b. Compliance with relevant laws, standards, and regulations.
 - c. Careful selection and management of CSPs and other components within the system.



- d. Data classification, storage, access controls, data retention policies, and data sovereignty.
 - e. Continuous monitoring and evaluation of cloud operations to ensure ongoing compliance, security, and optimization.
3. Focus on continuous improvement of controls and policies based on cloud practices and find areas or gaps for improvement.

Roles and Responsibilities

Clear delineation of roles and responsibilities is always critical. With the cloud, roles and responsibilities can change or emerge. See [Appendix 3: Sample Cloud RACI Chart](#) for a comprehensive list of roles and responsibilities created by a large federal agency.

Change Management

An existing change management structure is likely in place for all agencies. This process is probably aligned with the traditional cadences of an on-premise or data center operation.

For cloud operations, this traditional approach may not accommodate the dynamic qualities of the cloud. For example, depending on the operating model (see [Selecting an Operating Model](#)), development teams may have control over a particular segment of the agency's cloud. Alternatively, the cloud service may automatically create or delete resources depending on demand. Finally, the use of DevSecOps and Agile methodologies needs a change management model that supports faster and shorter cycles.

A comprehensive audit trail of the deployment steps can be achieved by using policy and automation for governance in the cloud. Furthermore, agility involves not penalizing failures, but reversing changes that have adverse business outcomes. Agencies should use automation to assist with this process of rolling back changes.

Whether cloud or on-premise, the core value of a change management process remains the same. These values include ensuring systems are stable and secure, creating clear communications and collaboration between various stakeholders, and providing a process to manage requested changes.

Below are some considerations with respect to managing change with a cloud infrastructure. See Figure 10: Sample Change Management Process.

Self-Managed or Automated Policy Checks

Self-managed changes are more agile as they require fewer approvals. Self-managed changes reflect lower-risk changes that follow a well-documented process and have a risk mitigation strategy. These changes may occur regularly and might include activities like minor upgrades or patching for certain systems. This approach is biased towards change enablement and requires a shift in mindset because it creates more autonomy for engineering teams.



Similarly, change management can leverage automated policy checks (see figure 12). This approach accelerates the approval of certain types of changes based on existing policy. It reduces human intervention while still maintaining the appropriate audit trail for compliance checking, performance, and possible rollbacks.

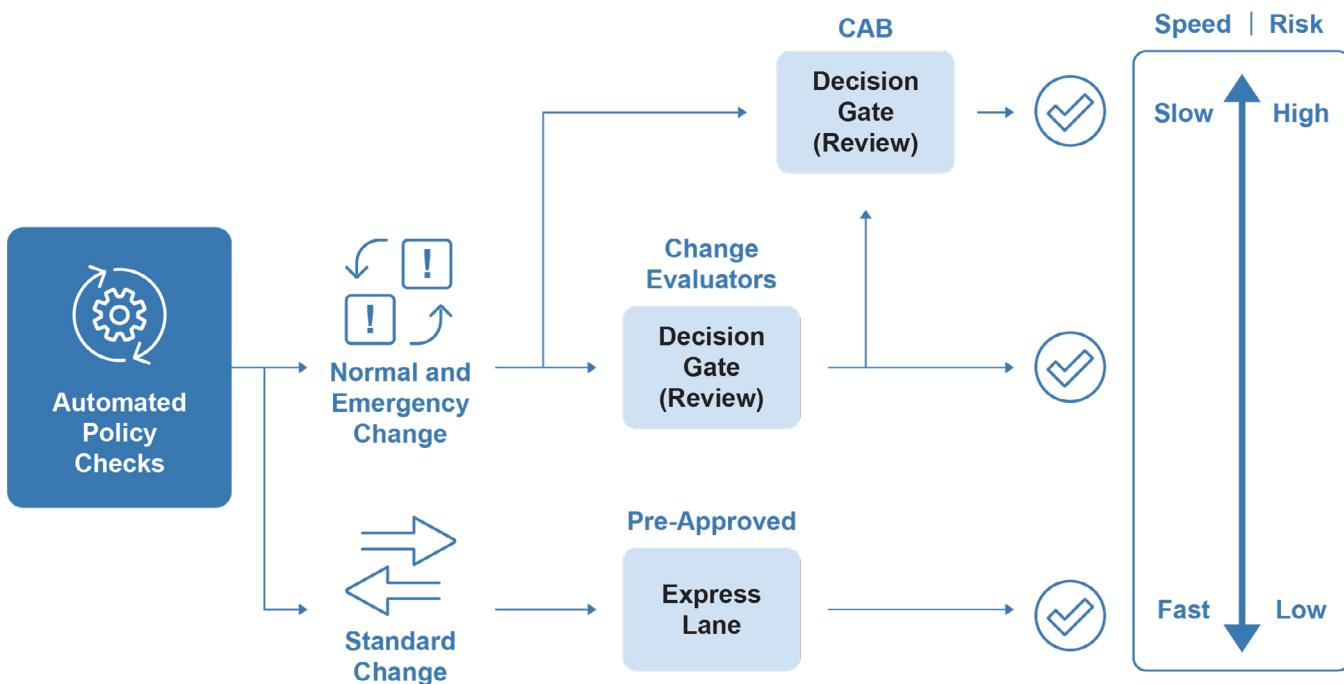
Implement Standard Changes

Introduce standard changes as a pathway for swift and safe changes. In this context, standard changes operate without decision gates that can impede or alter the course of change. The standard change would likely be a well-known task with a known (low) risk profile and may require an associated protocol to be performed as due diligence. One example might be standard patch cycles used by many vendors.

However, the express lane is not applicable for normal and emergency changes due to their elevated risk rating. Consequently, these types of changes must undergo evaluation at the appropriate decision gates. To determine the appropriate change path, an automated policy check should be utilized. The primary objective is to facilitate the transition of as many changes as feasible to the low-risk lanes.

Figure 12: Sample Change Management Process

Goal should be to move as many changes to low risk lanes as possible





PORTFOLIO MANAGEMENT & RATIONALIZATION

The agency application and technology portfolio should align with the agency's cloud strategy to maximize the value and effectiveness of the portfolio and to minimize complexity and costs. Establishing a detailed inventory of your agency's application and technology assets supports this goal. With an enterprise-level inventory, an agency can determine business value, quantify total cost of ownership, and identify whether any given asset belongs in the cloud. Not all tools or services may belong in the cloud. Rather, a key outcome is to establish a shared understanding of what should and should not be in the cloud.

Successful portfolio rationalization efforts require support from key stakeholders across the enterprise and include senior leaders, IT staff, cybersecurity experts, mission and program owners, financial practitioners, acquisition and procurement experts, and end user communities.

Once stakeholders are identified, the agency should establish a baseline inventory. This is followed by an environmental scan to identify applications and other technology resources to capture relevant data pertaining to each resource. All data should be validated and analyzed to identify the business value and technical fit of each resource. The total cost should be assessed and then each asset scored based on value, technical fit, and total cost. Finally, next steps should be established to determine the appropriate actions and sequence. See Table 5 for the possible cloud migration scenarios.

The process above is outlined in detail in the [Application Rationalization Playbook](#) and represented in Figure 13. Note that, while this playbook is focused on business applications, this general process would apply to any potential IT service or resource.

The Application Rationalization

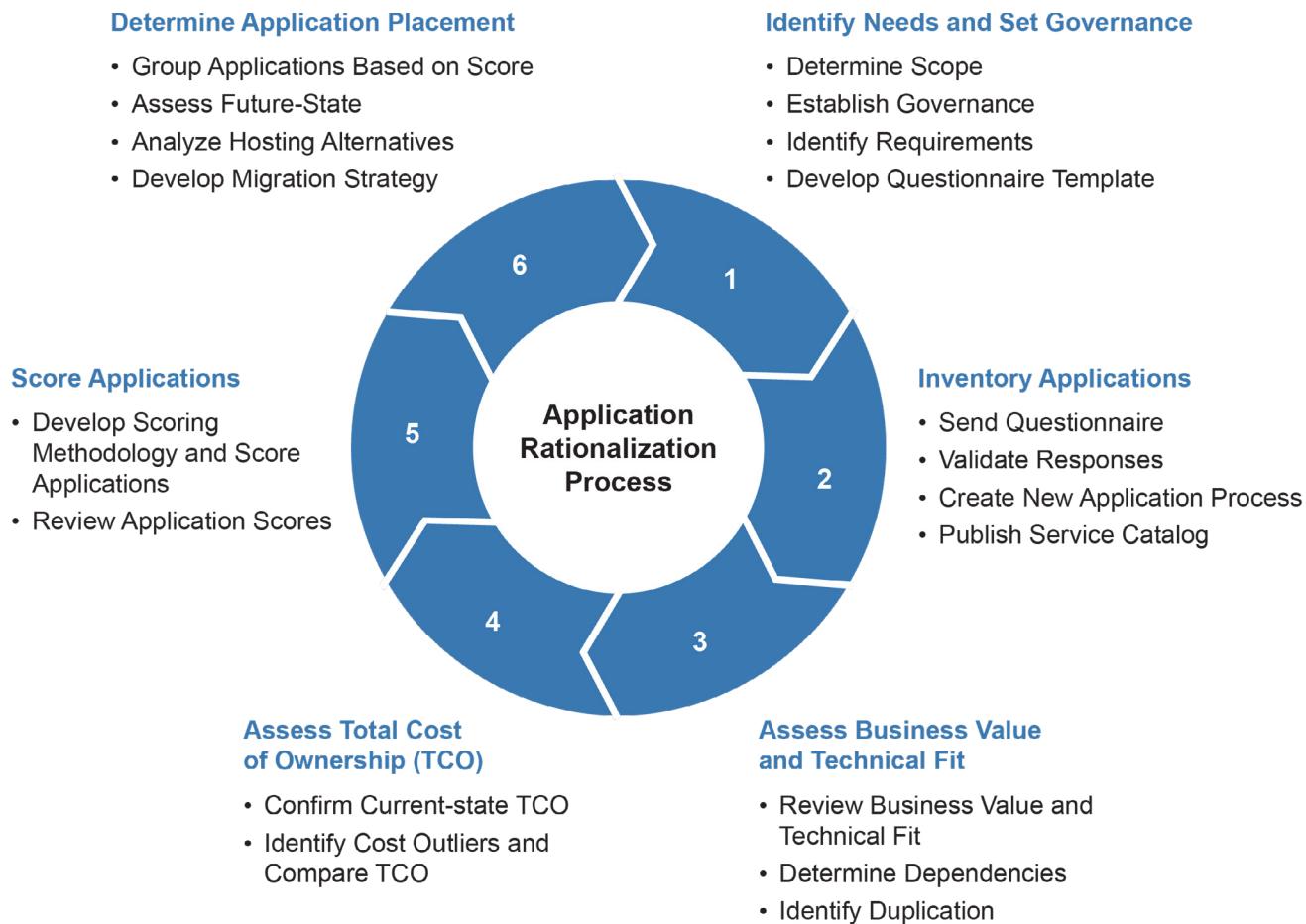
PLAYBOOK

An Agency Guide to Portfolio Management





Figure 13: Application Rationalization Process



As a starting point for how your agency should think about its applications and technology resources, consider the questions below to better understand the business value and technical fit for each.

- What is the name of the resource or application?
- What are its functions? How is it characterized?
- Who is the owner? Who are the users?
- Was it purchased or custom built? Is it a packaged application from a vendor?
- Who created or implemented it? Was it in-house or contracted?
- What are its dependencies?
- What version is it?
- Is it End-of-Life or End-of-Service?
- Is it currently virtualized?



- What are the security, governance, and data requirements?
- Does it have special geographic location requirements?
- Does it have a valid authorization to operate (ATO)?
- What is its assessed impact level (high, moderate, low)?
- Does it have personally identifiable information?
- What are the current and expected demands? Are these demands constant or changing?

Once your rationalization is complete, determine your management approach to a potential cloud migration for the application or resource. Standard approaches for workload or application disposition include retain, rehost, refactor, revise, rebuild and replace.

Table 5: Possible Migration Scenarios

Migration Strategy	Description	Benefits/Challenges
Retire	Remove application from infrastructure. Properly adjudicate data.	No new costs. Opportunity to streamline infrastructure and remove unnecessary workloads.
Retain	Leave resources or applications. Do not migrate to the cloud.	No new costs, but opportunities to leverage benefits of the cloud are lost.
Rehost	Redeployment of the workload to a new environment. The workload continues to retain many of the same features as it did in the old, on-premise environment (i.e., lift-and-shift).	Rehosting can theoretically be done quickly by simply moving a legacy workload to the cloud, but that shift risks performance problems when the workload cannot meet the demands of a cloud environment (e.g., by scaling on demand).
Refactor	Partial modification of the code used to run an existing workload, such as the replacement of one of the application's original components with a cloud-native tool.	Refactoring can be done using coding languages, containers, etc., that developers are familiar with. However, existing workloads cannot necessarily all be modified in such a way that they can take advantage of all cloud aspects.
Revise	Heavy modification of the code used to support an existing workload. The code modification makes it possible to later rehost or refactor the workload in the cloud.	Higher costs and more time consuming compared to rehosting or making minor changes to the code.



Migration Strategy	Description	Benefits/Challenges
Rebuild	Rewrite an application's code to enable it to move from its existing infrastructure host to a Platform as a Service solution.	A workload re-architected to operate on a CSP's platform can take advantage of the PaaS's features, although rewriting code beforehand requires significant investments of time and budget.
Replace	The existing workload is abandoned in favor of a new solution with cloud or on-premise delivery. (Includes both custom developed software or commercial-off-the-shelf COTS software)	Investing in SaaS solutions can reduce or remove the need for a development team focused on the workload. Lack of customization could risk creating challenges with vendor lock-in or data accessibility. For custom development, costs will be much higher and reflect ongoing Operations and Maintenance (O&M) activities. In theory, custom work delivers the necessary functionality.

WORKFORCE PLANNING

As agencies modernize their IT infrastructure, there are key questions they need to ask. Can you support the cloud with what you have? If not, do you upskill your existing staff, hire new staff, or outsource? Key considerations include:

- Cloud operations can introduce **new operating models** that change roles and responsibilities.
- Competition for **technical resources** is aggressive and new approaches may be warranted.
- Cloud operations usually require **new skills** for teams and contractors, and existing skills for one cloud provider may not be sufficient for a new provider.

Finding Technical Resources

Assessing your technical needs is an important step as you build or expand your cloud investments. The Office of Personnel Management (OPM) has identified the critical competencies and tasks employees need to perform successfully in nearly 200 federal occupations. Review the [OPM Competency Models](#) for IT program management, cybersecurity, and more. See [Appendix 4 for select cloud roles and descriptions](#) that may apply directly to your cloud operations team.

Hiring the right resource can be difficult as well as expensive in the best of circumstances. With long hiring lead times, federal agencies are at a disadvantage. Creative approaches may be needed to fulfill expected operational needs, such as using different hiring authorities, hiring people earlier in their careers and providing training, and identifying existing staff who are a good fit.



Ideal Cloud Skill Sets

Agencies should focus on the following skill sets when hiring or training the staff required for an IaaS environment.

- Site Reliability Engineering (SRE). SRE is a generally recognized IaaS organizational role. SREs require a broad skill set and are best suited for more complex operations like distributed cloud environments or developer-based operations. SREs are typically cloud platform experts who have strong foundational knowledge in automation and software engineering. They understand Infrastructure as Code, networking fundamentals, and how to design scalable architectures to support varying workloads and traffic patterns. They are problem solvers who do well in distributed environments.
- Programming. Programming and scripting skills are necessary for managing, developing, and deploying applications and services within an IaaS environment. This skill is vital for implementing automation and supporting IaC. Also important is the need to develop and maintain code in a disciplined manner. Without this essential rigor, technical debt will accrue and create systems that are more difficult to maintain and optimize.
- Platform Expertise. Every IaaS platform has unique features, services, and tools. Ensure your employees have training or experience with your agency's cloud service providers.
- Selecting Cloud Services. Your cloud team needs to have the ability to choose the right services for your agency. This can be knowledge on which services to leverage for specific use cases (e.g., compute, storage, networking, database, etc.).
- Cloud Integration and Management. If your agency uses multiple IaaS solutions, ensure your team members have knowledge and skills to integrate different services. Your team will need to manage multiple vendor platforms, monitor, and troubleshoot incidents.
- Cloud Security and Compliance. Your team must be familiar with unique security considerations and be familiar with the cloud shared responsibility model.

Training

Whether training staff to learn a new job or keeping your staff up to date, your agency should consider training a recurrent obligation. Training will ensure IT staff are current in the latest technology, internal processes, policies, and relevant architecture or systems.

Consider providing more training at the start of employment to build the necessary skills. Look at both upskilling existing staff and investing in new workforce entrants to establish the needed skills.

The [CIO Council Cloud and Infrastructure Community of Practice Training](#) offers a limited number of no-cost trainings.



SUSTAINABILITY

IT Sustainability is an emerging interest that addresses the environmental and social impacts of IT operations and the responsible use of technology resources. Optimizing cloud resources equates to lower power consumption and a reduced environmental impact. Typical interest areas include energy efficiency, e-waste, procurement, and resource consolidation. The IT Sustainability Best Practice Guide provides further guidance.

One strategy is to pick hyperscalers and locations based on its use of alternative energy sources. Many cloud service providers provide dashboards to show carbon footprint or data center power sources.



SECURITY

"By 2022, 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the UI, up from 40% in 2019." (Gartner)

Securing IT services is an ongoing obligation of every federal agency. The use of cloud services does not change an agency's obligation to manage the confidentiality, integrity, and availability of data and systems.

Cloud security, like any federal IT security issue, is mandated by the [Federal Information Security Modernization Act](#) (FISMA). The [National Institute of Standards and Technology](#) (NIST) provides the standards. The [Cybersecurity and Infrastructure Security Agency](#) (CISA) provides technical guidance to support implementation. The [Federal Risk and Authorization Management Program](#) (FedRAMP) authorizes services that can and should be used by all federal agencies. Finally, agencies need to have their own policies and procedures to define internal operations. See Figure 14.

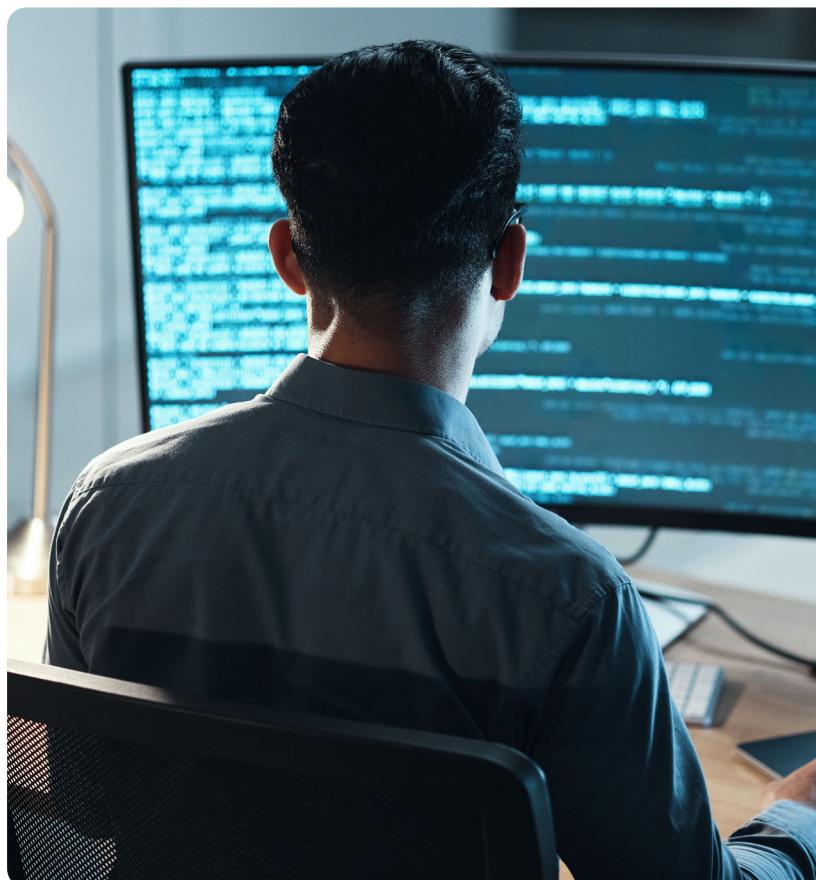




Figure 14: Building Blocks for Operational Security



The following themes should be considered as you review these best practices:

- In addition to being well documented, good operational security requires consistent execution and continuous monitoring.
- Governance is important! Security practices need to be audited and updated to reflect due diligence, new technology, and emergent risks.
- Training is necessary. Simply, how can your agency effectively secure a service if your operations team is not proficient in its use?



CLOUD AND ON-PREMISE DIFFERENCES THAT IMPACT SECURITY

The unique benefits of the cloud bring new operational challenges from a security perspective. These include:

- **Robust monitoring.** With the cloud, telemetry is built in and the volume of potential data may exceed prior experience and current methodologies for analysis.
- **New roles and responsibilities.** Your traditional security team may need training and have updated responsibilities.
- **Security is a shared responsibility.** The mix of shared responsibilities depends on the service and its implementation.
- **New services can be quickly provisioned.** This capability can address demand fluctuations but also increase attack surfaces and add unknown elements to your system.
- **Data is off-site.** In the cloud, CSPs typically provide encryption mechanisms for data at rest and in transit, but customers must manage access controls and encryption keys effectively to ensure data security.
- **Incident response is shared.** Agencies must work closely with the CSP to define roles and responsibilities during security incidents and understand how incident response procedures are coordinated between the customer and the CSP.
- **Changing network boundaries.** On-premise security often relies on network perimeters and firewalls to secure internal networks. In the cloud, the focus shifts to securing individual resources and data at a more granular level as there is no clear network boundary due to the distributed nature of the cloud. See [Zero Trust](#).
- **Identity and Access Management (IAM).** IAM involves managing user access, authentication, authorization, and encryption keys. Cloud providers offer IAM services to control access to resources, enabling agencies to implement least privilege principles and fine-grained access controls.
- **Leveraging automation and orchestration.** Unlike on-premise security that may rely on manual processes, efficient cloud environments leverage automation and orchestration. Security measures should align with this approach by automating security configurations, implementing continuous monitoring approaches, and using DevSecOps processes to test and implement changes.

CHANGING AGENCY RESPONSIBILITIES

Whether formally-approved through FedRAMP or requesting an exception using the required FedRAMP baselines, the agency is ALWAYS responsible for the security of the system.

This is as true for SaaS as it is for an IaaS or PaaS. The definitive guide on security controls is the [NIST 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations](#).



FedRAMP provides a baseline of security controls; however, agencies are encouraged to look carefully at the customer responsibilities matrix to determine exactly which controls they are responsible for and which controls they can inherit from the cloud provider.

Use the CISA [Cloud Security Technical Reference Architecture](#) to provide a comprehensive overview of cloud security with recommendations for approaches to cloud migration and data protection for agency data collection and reporting.

For an exhaustive review on managing enterprise risk, please see the [NIST 800-37 Rev 2, Risk Management Framework](#).

CUSTOMER RESPONSIBILITY MATRIX

The agency, not the vendor, is responsible for vetting the security of the system using established baselines. As early as possible, the agency should require any cloud provider (whether SaaS, PaaS, or IaaS) to provide a customer responsibility matrix. A customer responsibility matrix outlines the specific security and operational responsibilities of the customer or client using cloud services. It clarifies the areas where the customer holds primary responsibility for implementing and managing security controls, compliance measures, data protection, access management, and other related aspects within the cloud environment.

Identifying this division of labor should happen as early as the acquisition lifecycle. Clearly and promptly establish these obligations to ensure optimal outcomes for cloud operational efficiency and effectiveness. Discovering a deficit in controls or simply struggling to understand the best answer will always be hardest if it happens during implementation.

If the cloud product is FedRAMP authorized, then request the Control Implementation Summary that is created as part of the approval process. See [FedRAMP](#).

ASSESSMENT & AUTHORIZATION

Assessment and authorization (A&A) is a comprehensive evaluation of an agency's information system policies, security controls, policies around safeguards, and documented vulnerabilities. Given the level of effort to conduct an A&A, preparing for this process should begin at the earliest stages of acquisition planning.

Authorization to Operate

An Authorization to Operate (ATO) is the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems. [See OMB Circular A-130 \(7/28/2016\)](#).



Bear in mind that the ATO is not the final step. Rather, it provides the starting point for authorized product use and initiation of continuous monitoring. Changes to any system, including cloud-based systems, must be vetted as part of the continuous monitoring process.

The appropriate response to a given change will depend on the significance of the change itself and your agency's risk management profile. Possible responses include waiting for the schedule reauthorization. Communicate with your security team to understand and plan for the appropriate response.

FedRAMP

All federal agencies shall “use FedRAMP when conducting risk assessments, security authorizations, and granting ATOs for all Executive department or agency use of cloud services.” ([Security Authorization of Information Systems in Cloud Computing Environments](#), Section 4. d. i.)

The [Federal Risk and Authorization Management Program](#) (FedRAMP) accelerates the adoption of cloud computing by allowing agencies to leverage A&As on a government-wide scale. This program prevents agencies from recertifying the same cloud product. This “do once, use many” approach reuses standardized security assessments to save agencies time and resources. Agencies can save money and time by adopting cloud services that are already FedRAMP authorized because the overall authorization level of effort is reduced.

Whether IaaS, PaaS, SaaS, or some combination, agencies must ensure their cloud products or services comply with FedRAMP. A vendor cannot authorize a system. The agency has the responsibility to ensure all appropriate controls are in place. Your agency should have appropriate policies in place to ensure all cloud services are properly authorized.

The first option is to leverage **FedRAMP-Ready** or **FedRAMP-Authorized** services. Note that a FedRAMP-Authorized service indicates that the CSP's security package is available for agency review and reuse, whereas FedRAMP-Ready indicates a service that is ready to begin the authorization process. See the [FedRAMP Marketplace](#) for details on these different designations. A second option is to sponsor a preferred provider as part of a FedRAMP authorization. See [FedRAMP](#) for additional information. As a final option, an agency can request an exemption. See the [Security Authorization of Information Systems in Cloud Computing Environments](#), Section 4(d)(vii) for more information. This does **not** exempt the agency from securing the system. In fact, the FedRAMP-approved baselines must still be implemented. Also, identifying the authorization boundary that is provided in the FedRAMP-Authorization package is critical. It is very important the Agency clearly understands what services from the CSP are included. See Table 6.

**Table 6: Assessment & Authorization Approaches**

Step	Approach
1	Use a FedRAMP-Authorized service and re-use its security package as part of the Agency's ATO.
2	Select a FedRAMP-Ready service to achieve a FedRAMP-Authorized designation and Agency ATO, or sponsor a CSP for FedRAMP-authorization.
3	Establish vendor, shared and agency-responsible controls. Conduct the necessary verification procedures, develop an System Security Plan (SSP), and implement the service with FedRAMP-compliant controls.

The FedRAMP office provides agencies and cloud vendors with security templates that can be used with Low, Moderate, or High impact cloud offerings. See [Understanding Baselines and Impact Levels in FedRAMP](#) for more details on impact levels. Use the appropriate template and adapt your agency's specific controls based on mission and risk tolerance.

As part of your evaluation, request the Control Implementation Summary (CIS) from your vendor. CSPs are required to submit a CIS Workbook as Attachment 9 to the FedRAMP SSP template. The CIS Workbook includes a Customer Responsibility Matrix (CRM) and CSPs must use the CRM to describe the specific elements of each control where the responsibility lies with the customer. See [FedRAMP CIS Sample workbook](#) for the template used for the CIS.

Additional relevant FedRAMP resources include:

- [Listing of FedRAMP-authorized, -ready, and -in process products](#)
- [FedRAMP Agency Authorization process](#)
- FedRAMP SSP templates for [Low baseline, Moderate baseline, and High baseline](#) impact levels.
- [FedRAMP FAQs](#)

Automating Security Operations

The process leading to an ATO and the processes associated with continuous monitoring often require a significant investment of time and resources. Automation can be useful with assessment, monitoring, and authorization activities. It can also enforce standards and generate an audit trail. The marketplace is developing products to support these types of automation.

At present, likely no end-to-end automation solutions can address all of an agency's needs. However, consider leveraging tools to automate steps within your workflow. Look to [DevSecOps](#) for a framework that integrates well with cloud operations. This framework emphasizes automation as well as culture and design to integrate security throughout the IT lifecycle. Code scanning, workflow scans, runtime scans, and environment scans are often a part of this approach. See Figure 15.



Leadership



Management



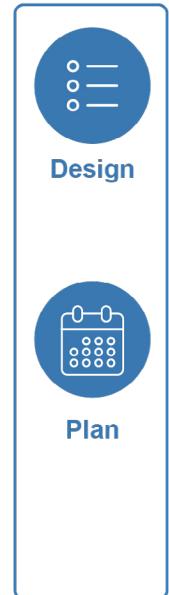
Security



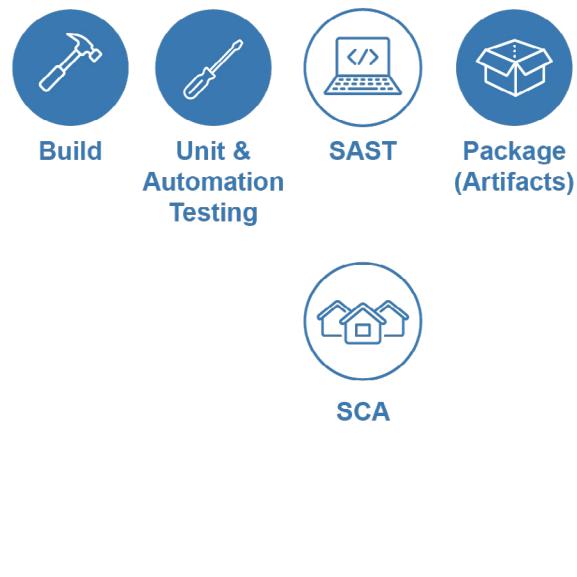
Engineering

Figure 15: Sample DevSecOps Pipeline Approach

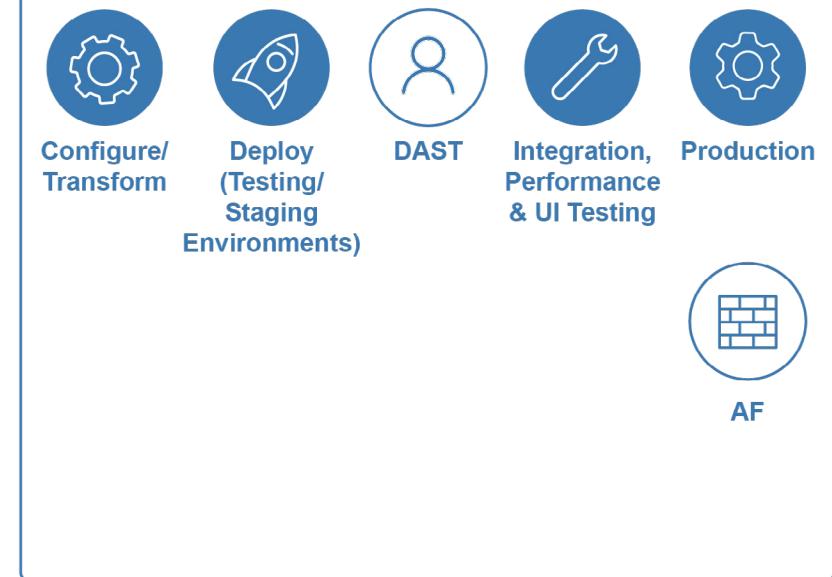
Continuous Integration



Commit or Pull Request (Merge)



Continuous Delivery & Deployment



Threat Modeling



Logging and Monitoring



DevOps Pipeline



DevSecOps Pipeline

DAST- Dynamic Application Software Testing

SAST- Static Application Software Testing

SCA- Software composition analysis

WAF- Application Firewall



[Open Security Controls Assessment Language \(OSCAL\)](#) is a relatively new effort from NIST that supports more robust security-related workflow systems. This language provides machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results. This transparent and transactional format supports the automation of control-based risk management like the implementation of 800-53. There are products that support OSCAL in this evolving market.

The Continuous Authorization To Operate (cATO) is also an evolving effort to apply agile process frameworks to the assessment and authorization process. Through its engagements with other federal agencies, the GSA Cloud Center of Excellence has developed best practices based on cATO principles. Key practices include:

- **Continuous Monitoring.** Priority should be placed on automation for compliance and reporting. Tools that cannot support automation of compliance functions or updates to key evidence should be considered end-of-life and replaced as soon as practical.
- **Active Cyber Defense.** Agencies should move from static assessments and reactive postures to active assessments and predictive postures. Mature cyber security capabilities include adoption of predictive threat models. Agencies should develop and integrate threat modeling processes into predictive analytic practices capable of anticipating and preventing potential attacks against information systems.
- **DevSecOps.** Build continuous delivery pipelines using the DevSecOps framework as a starting point. Agencies are encouraged to embrace Infrastructure-as-Code routines, and add security checks, tests and gates into application and infrastructure pipelines.

MONITORING

Monitoring and scanning should be done on any IT platform – cloud or on-premise. Monitoring observes and tests applications, services, traffic and other activity to identify potential flaws or problems. Tools are required to effectively conduct this type of monitoring; this is especially true with a cloud environment.

CSPs (at the IaaS-level) will likely provide a cloud-native solution to support these functions. While there are many third-party products to support this necessary function, the first choice is to use the vendor's tool to manage, monitor, and assess the environment.

Monitoring tools may be more significant for agencies with a multi-cloud ecosystem since using different cloud-native solutions may require different training and make collating data challenging. See [Multi-Cloud and Hybrid Cloud](#). Such agencies may explore third-party options to provide a unified platform to support different CSPs. However, compatibility issues may challenge the desired goals. For agencies that are pursuing a unified view of multiple clouds, ensure your testing and requirements align with your needs and wants.



SUPPLY CHAIN RISK MANAGEMENT

Agencies must manage supply chain risk. This is not only a best practice but a requirement as outlined in OMB M-22-18, [Enhancing the Security of the Software Supply Chain through Secure Software](#). Given the many complicated relationships that can form a supply chain for any given vendor, this can be challenging to put into practice.

Conducting Supply Chain Risk Management (SCRM) is difficult because this information is not readily available across the chain of relationships, services and goods that make a vendor's services possible. Additionally, the available resources within any given agency, as well as the established risk tolerance, must also be taken into account to understand the due diligence appropriate for your agency.

Also, align your SCRM strategies with the planned implementation of identity management that also enables streamlined adoption of zero trust principles such as segmentation. Zero trust offers a framework that helps mitigate bad actors by limiting or eliminating the potential for damage to the overall network.

Consider the following areas for your SCRM tactics:

- Establish a policy to ensure that all new entrants to your cloud environment must go through your established change management process. Connectors, plugins, open source software, and scripts all present opportunities to introduce elements that may be malicious at worst or unreliable at best. Products that are not supported by larger vendors may be particularly hard to evaluate. Everything, including components embedded within systems, should be vetted.
- Integrate SCRM due diligence into the overarching governance process. This could include a policy statement that outlines the agency's expectations as well as incorporating basic investigative questions about a new tool. See Appendix 5: [Change Management Process and Questions to Support Supply Chain Risk Management](#).
- When making purchasing decisions for new products, consider establishing preferences for sourcing. This approach builds on existing trusted relationships first, then looks at other options. An example of a rank-ordered set of preferences are below:
 1. Using FedRAMP-Authorized products.
 2. Using the Marketplace associated with established FedRAMP providers.
 - a. This approach does not mean you are buying FedRAMP's product, but rather using an existing, vetted supplier for your requirements.
 3. Using products on the open marketplace including open source software.
- Be transparent with your portfolio of products used in the cloud. Everything should be documented to include the various libraries and modules used in software development.
- Ensure the applicable points of contact (POCs) in finance and acquisitions are conversant with the implications of new software and how it can change the risk profile of the overall IT systems and agency mission.



- Be advised that mobile apps used in conjunction with cloud services may not connect to the government version of the cloud. Rather, the apps may connect to the commercial entity, and therefore non-FedRAMP'd, service.

Additional resources include:

- [FTC Vendor Security](#)
- [Supply Chain Risk Management: Reducing Threats to Key U.S. Supply Chains \(DNI\)](#)

ESTABLISHING DIGITAL TRUST

Identity is the foundation to security because it establishes digital trust both on-premises and within cloud environments. With identity management, you authenticate users. With access management, you authorize users for resources.

Identity management focuses on managing the attributes related to the user, such as their name, role, login credentials, etc. It also entails creating and maintaining digital identities for every user or entity on a network.

Access management focuses on evaluating the attributes based on policies and making yes or no decisions about granting access to network resources (e.g., apps, data, or services). It includes enforcing access permissions based on the user's role or other criteria. Typical functions include managing users, groups, and permissions.

Trust Management Playbooks

In-depth resources to support agency identity and management efforts are available from [idmanagement.gov](#). These digital identity playbooks offer technical guidance, provide implementation approaches, and offer strategic advantage to securing identities within their missions. Playbooks help train staff and can accelerate agency identity and access implementations. The following highlights specific playbooks to get started:

Digital Identity Risk Assessment

The [Digital Identity Risk Assessment](#) playbook should be consulted early in an agency's identity management process. Risk assessment helps agencies make informed decisions about asset management and digital trust. These assessments will help prioritize identity and access management efforts. Digital authentication provides reasonable risk-based assurances that the individual accessing the application is the same individual who previously accessed the service. This playbook applies to the [NIST Special Publication 800-63-3](#) digital identity guidelines. Leverage this playbook as part of agency risk assessment early in the process.

Cloud Identity

The [Cloud Identity Playbook](#) assists federal agencies in workforce identity credential and access management services within a cloud model. The playbook highlights a four-step process to initiate or expand workforce identity access management services in a cloud



operating model. This playbook was created in collaboration with the federal Chief Information Security Officer Council Identity Credential and Access Management subcommittee and the federal Chief Information Officer Council Cloud and Infrastructure Community of Practice.

Privileged Identity Management

The [Privileged Identity Management Playbook](#) helps agencies protect their high profile users and accounts. Privileged accounts typically have elevated rights to systems, applications, and data. Elevated rights for privileged accounts often present an attractive target to adversaries. Unwanted behavior or compromised privileged accounts are responsible for the most cybersecurity incidents globally. Agencies should leverage this playbook to secure their privileged accounts early and defend agency assets. This playbook was created in collaboration with the General Services Administration Office of Government-wide Policy Identity Assurance and Trusted Access Division, the Federal Chief Information Security Officer Council ICAM Subcommittee, and the Department of Homeland Security Cybersecurity and Infrastructure Security Agency Continuous Diagnostic and Mitigation Program.

Digital Worker Identity Playbook

The [Digital Worker Identity Playbook](#) is a practical guide for managing so-called “digital workers.” A digital worker is an automated, software-based tool, application, or agent that performs a business task or process similar to a human user and uses AI or other autonomous decision-making capabilities. This playbook is relevant to cloud environments in which automation plays an important role. This playbook helps agency ICAM programs, cloud operation teams and CIO and CISO offices determine the risk of and define a process for digital worker identity management. This playbook is a collaboration between the Identity Credential, and Access Management Subcommittee of the Federal Chief Information Security Officer (CISO) Council and the General Services Administration Office of Government-wide Policy Identity Assurance and Trusted Access Division.

For more identity and digital trust playbooks and policies such as [Identity Lifecycle Management](#) and [Windows Hello for Business](#), please visit the [IDManagement.gov](#) website

SECURE CLOUD SERVICE CONFIGURATIONS

All agencies need to ensure their cloud services are secure regardless of their FedRAMP status. Even if a product is FedRAMP-Authorized or FedRAMP-Ready, your agency must secure the service with the appropriate controls and settings. Refer to the [Customer Responsibility Matrix](#) section for thoughts on identifying controls that are inherited (e.g., managed by vendor), shared, or the customer’s responsibility.

There are some useful benchmarking resources for configuring specific systems or products. However, with so many new and updated products, a definitive source for the appropriate configuration setting to implement a control often does not exist.

A few resources are noted below. These resources offer a starting point for securing, or hardening, your cloud-based service. Regardless of the source, these benchmarks are only a starting point



as appropriate due diligence will require an agency to comprehensively evaluate and adapt the benchmark to reflect its particular needs and risk tolerance. Be sure to integrate any updates to the system within your agency's existing change management process.

- **Cloud Service Provider Documentation.** Most CSPs offer detailed guidance and best practices for securing their services. These resources often include security configuration recommendations, access controls, encryption options, network security, and more.
- **Cloud Security Frameworks.** Various cloud security frameworks provide guidelines and best practices for securing cloud environments. For example, the [Cloud Security Alliance](#) has the [Cloud Controls Matrix](#) that offers a detailed framework for assessing and implementing security controls across different cloud service categories. Also, agencies such as the National Institute of Standards and Technology ([SP 800-53](#)) and the International Organization for Standardization (e.g., [ISO/IEC 27017](#)) publish guidelines and standards that can help you establish secure configurations.
- **Third-Party Hardening Guides.** Third-party organizations create security hardening guides for specific services or platforms. These guides provide step-by-step instructions for securing various components of the cloud environment, including network configurations, access controls, encryption, and logging. These include:
 - [Secure Cloud Business Applications \(SCuBA\)](#) (CISA)
 - [Center for Internet Security](#) (Private Sector)

API SECURITY

As agencies leverage more cloud services and create cloud native applications, it is critical to consider the security implications of Application Programming Interfaces or APIs. APIs are a standard approach for cloud-based applications and microservices to interface or communicate with other services. Their ability to read, update, or delete data can pose significant security risks without the appropriate precautions. It is vital that security and engineering teams are collaborating on the best approach for safeguarding API communications. While specific security recommendations are out-of-scope for this document, the following guidelines are a good starting point.

- Document all APIs and their purpose
- Map connection points, owners and potential risks
- Monitor and report at the API-level where possible
- Identify security risks associated with APIs
- Consider using API gateways to manage and secure traffic





ENCRYPTION

Encryption is a key security component of any information system. While any likely cloud-based solution will have encryption of some sort, it is incumbent on the agency to ensure the provided encryption is sufficient for its needs. Also, an agency may be responsible for configuration and management. See CISA's [Operational Best Practices for Encryption Key Management](#) and Table 7 for best practices. Particularly, the management of encryption keys may be vital in using best practices to manage and store this critical information. Please see [NIST 800-57 Recommendation for Key Management](#) for detailed guidance.

Table 7: Encryption Best Practices

Recommendation	Description
Use Strong Key Management	Ensure your agency uses industry standard and NIST-recommended encryption keys such as AES.
Rotate Encryption Keys	Define key rotation procedures. Key rotation is the process of retiring an encryption key and replacing it with a new encryption key.
Secure Key Storage	Use secure and redundant storage for the encryption keys. Ensure the environment offers strong management controls including access controls, encryption at rest, and backups.
Key Isolation	Encryption keys must be stored separately from the encrypted data. It is recommended to store the encryption keys in a hardware security module or another separate physical location with strong physical and logical protections.
Encryption Key Lifecycle Management	Implement a well-defined key lifecycle management process. This includes key generation, distribution, usage, rotation, archival, and destruction. Clearly define roles and responsibilities for key management activities to maintain accountability.
Access Controls	Use strong authentication and multi-factor authentication. Access should be limited to key-authorized personnel only.
Monitoring and Auditing	Ensure you implement proper governance and oversight procedures by monitoring the use of the keys, any changes that transpire, and any access attempts.
Backup and Recovery	Implement routine backup procedures for encryption keys. Ensure your agency has detailed disaster recovery procedures for encryption key availability during system failures or disasters.
Testing keys	Implement periodic tests to evaluate your key management processes. Use vulnerability assessments to validate the effectiveness of your key management controls.



ZERO TRUST

“Zero Trust” (ZT) is a relatively new approach to managing enterprise security. Unlike perimeter-based security approaches, this approach assumes there are no traditional network boundaries to define access. Rather, authentication and authorization are **continually validated** in order to access applications and data. ZT builds on data security concepts of least privilege and continuous access validation. Many of the major IaaS CSPs offer capabilities to implement a Zero Trust architecture.

Your organizational plan for using the cloud should leverage ZT principles. Using ZT is not only a best practice, but a mandate as well. See [OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles](#). The [CISA Zero Trust Maturity Model](#) is a great starting point, and also consider [NIST SP 800-207, Zero Trust Architecture](#).

Agencies should design their cloud environment with Zero Trust Identity Management principles in mind. IaaS environments can easily support microsegmentation, encryption, user-based policy controls and many other capabilities that are aligned to the [CISA Cloud Security Technical Reference Architecture](#). Reference the [GSA Cloud Identity Playbook](#) to better understand how you can leverage identity services to begin implementing your Zero Trust architecture.

Consider and leverage the [Federal Identity, Credential, and Access Management \(FICAM\) framework](#). FICAM is a comprehensive set of guidelines and standards developed by the U.S. Federal Government to support secure and efficient management of identity, credentials, and access to information systems. FICAM promotes a Zero Trust approach and facilitates the implementation of Zero Trust principles in cloud-based systems.

From a general security perspective, your target solution should support the following principles in your cloud environment:

- Make the network irrelevant for access-based decisions; access should not be based on which network is used to connect.
- Access should be based on criteria from users and devices.
- All access should be authorized, encrypted, and authenticated appropriately.

Although zero trust implementation is out of scope for this document, from a high level perspective, you can use the following steps as a guideline.

1. Define security perimeters. Document the boundaries of your IaaS environment. Understand access needs between segments. Capture information about virtual networks, subnets, security groups, etc.
2. Divide your Virtual Private Cloud (VPC) environments into logical segments to avoid lateral movements, and isolate environments as required.
3. Implement a strong Identity and Access Management solution. Leverage native IaaS provider capabilities as required. Ensure you plan to implement multi-factor authentication and focus on implementing least privilege policies.



4. Implement security controls to limit traffic within your IaaS environment. Leverage Access Control Lists, network security groups and firewalls to manage traffic.
5. Divide your IaaS environment into smaller security zones using micro segmentation principles. The end result should be an environment with granular security zones. Use solutions to enforce policies at the workload level.
6. Use logging to monitor your environment and leverage intrusion detection and prevention systems, security information, and event management tools to intelligently analyze user activity and network traffic into and out of your VPC.
7. Implement continuous authentication and authorization controls. This could include using attributes about the user and their role or the nature nature of the app, as well as time-based access or session timeouts. The key is to balance user experience and productivity with the appropriate controls.
8. Encrypt data in motion with NIST recommended encryption guidance; be sure to encrypt both storage of any kind and databases.

GETTING HELP FROM CISA

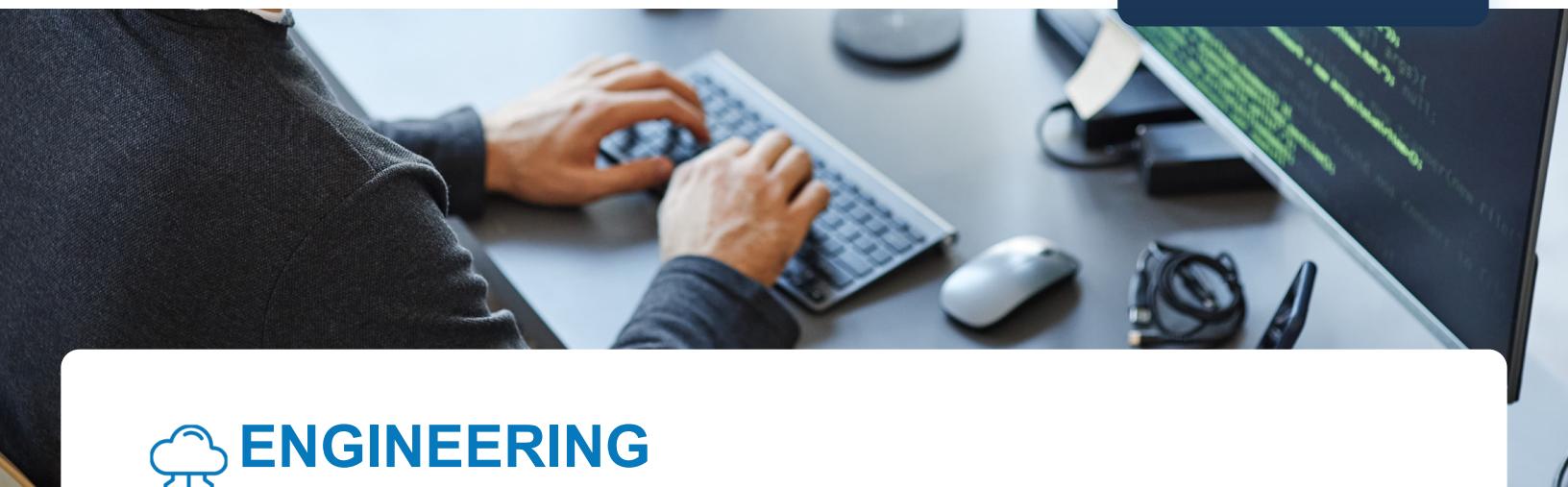
The Cybersecurity and Infrastructure Security Agency (CISA) offers a range of resources to support an agency's security journey. Beyond excellent guidance across a number of important cyber topics, CISA also provides direct support to address specific agency issues that includes assessments, vulnerability scanning, and resilience reviews.

CISA has its own continuous diagnostics and monitoring (CDM) program that provides tools and assistance in asset management, identity and access management, network security management, and data protection. CDM describes the effort to facilitate automated security control assessment and continuous monitoring by providing a comprehensive set of tools, dashboards, and assistance. See the CISA [Continuous Diagnostics and Mitigation \(CDM\) Program website](#) for more information.

Consider integrating your cloud with the CISA [National Cybersecurity Protection System](#) (NCPS). The NCPS offers agencies and the overall federal government intrusion detection, analytics, information sharing, and intrusion prevention. Agencies can submit their relevant log files via the [Cloud Log Aggregation Warehouse](#) (CLAW). CLAW is a CISA-deployed architecture for the collection and aggregation of security telemetry data from agencies. CLAW ingests, stores, and analyzes security and sensor data from agencies.

Other useful resources from CISA are noted below:

- [Cyber Resource Hub](#) (CISA) Enumerates the many services and resources available from CISA.
- CyberLiaison@cisa.dhs.gov A general email address to initiate questions or requests with the CISA support teams.



ENGINEERING

This set of best practices highlights technical considerations when operating a cloud environment.

When considering a migration or new deployment to the cloud, focus on requirements rather than attempting to replicate existing on-premise processes, procedures, approaches, and configurations in the cloud environment. Cloud usage offers technologies, solutions, and approaches that differ from what may exist on-premise. It is important to ensure those differences are considered not only when designing a system to be hosted in the cloud, but also for non-technical processes such as budget planning, usage tracking, support, monitoring, and so forth.

A paradigm shift is necessary when moving to the cloud from an on-premise data center. Your agency should frame this shift as an opportunity for transformation. As your agency modernizes, determine the best way to meet a requirement rather than adopting a “lift and shift” approach that replicates on-premise operations. Agencies may determine that an application or service should NOT move to the cloud and stay on-premise. See [Portfolio Management & Rationalization](#) for more details on assessing applications.

TARGET STATE

“If you don’t know where you are going, you’ll end up someplace else.” – Yogi Berra

Target states are unique to a given agency at a given time. Your target should be specific, measurable, and achievable. Your agency may begin relying on cloud-native technologies like microservices and automation to deploy and modernize its services. These elements may be key in achieving its next target. Possible targets include:

- **Initial.** At this stage, the agency has just started exploring IaaS cloud services and has limited automation capabilities.
 - Primarily using manual processes for provisioning and deployment
 - Human intervention required throughout all processes



- **Repeatable.** The agency has some experience with IaaS cloud and has automated distinct tasks within provisioning and deployment processes.
 - Beginning to adopt Infrastructure as Code practices to define and manage infrastructure using version-controlled templates
 - Automating the deployment of applications and services on the IaaS cloud using scripts or tools
 - Implementing basic monitoring and alerting systems to identify and respond to infrastructure and application issues
- **Defined.** The agency has established standardized practices and processes for leveraging automation in their IaaS cloud environment.
 - Adopting configuration management tools to automate the provisioning and configuration of infrastructure components
 - Implementing continuous integration/continuous delivery (CI/CD) pipelines to automate the build, testing, and deployment of applications on the IaaS cloud
 - Implementing auto-scaling mechanisms to dynamically adjust resources based on demand, optimizing cost and performance



- **Managed.** The agency has achieved a high level of automation maturity, with comprehensive management and optimization of their IaaS cloud environment.
 - Providing a self-service catalog for users to request and provision infrastructure resources, empowering teams to manage their own environments
 - Utilizing automation and monitoring tools to optimize cloud costs by identifying underutilized resources and right-sizing deployments
 - Automating compliance checks and security configurations to ensure consistent adherence to organizational policies and industry standards
- **Optimized.** The agency has achieved maximum automation maturity, leveraging advanced technologies and techniques to optimize their IaaS cloud environment.
 - Adopting DevOps and SRE practices to enhance collaboration, reliability, and scalability of applications and infrastructure



- Utilizing machine learning and AI technologies to automate decision making, predictive scaling, anomaly detection, and optimization of infrastructure and workloads
- Implementing automated remediation mechanisms that proactively identify and resolve issues in real time, reducing human intervention and improving system stability

Automation

When determining the level of automation your agency needs, you should account for the cost of implementation versus the expected benefits. Smaller operations with few repetitive tasks may not achieve the return on investment from automation. Furthermore, effective automation that is adaptable to a fast-paced environment may require a fresh look at the level of autonomy and current operating model. It is important to have a shared understanding of how automation is developed, used, and maintained.

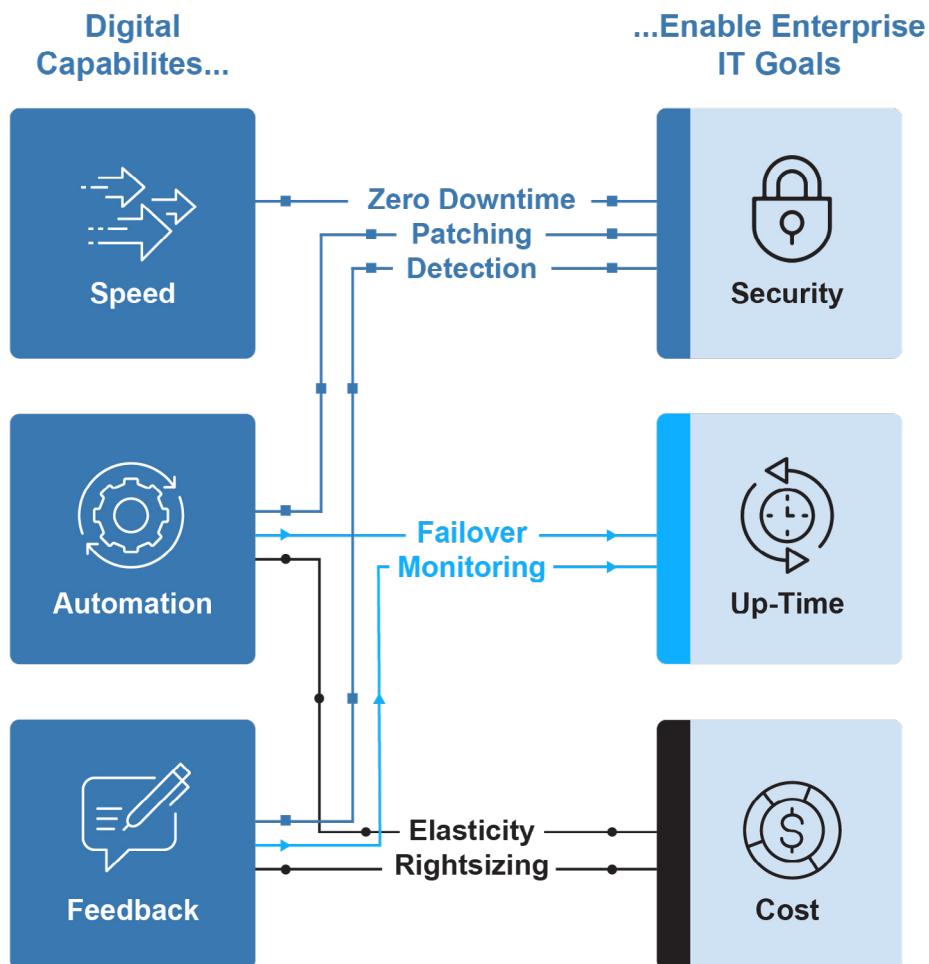
Automation may enable enterprise IT goals such as security, up-time, and cost. See Figure 16. Although automation may be a key enabler in achieving more efficient cloud operations, your agency should be mindful in how it implements new tools. Consider the following:

- Automating manual processes may obscure inefficient or ineffective steps within the process thereby missing further improvement opportunities. Automating poorly designed processes can amplify downstream challenges
- Automated processes may be “passed over” as done without due diligence for further analysis and improvement





Figure 16: How Automation Supports Effective Cloud Operations



PROVISIONING & DEPLOYMENTS

Provisioning and deployments are complementary processes in cloud environments. Provisioning sets up the infrastructure required to run applications. Deployments focus on deploying and managing the applications themselves. Automating these tasks can simplify and standardize all components of the cloud environment.

Provisioning refers to the process of setting up and configuring the underlying infrastructure required for running applications or services in the cloud. Provisioning tasks typically include activities like defining resource requirements, selecting appropriate instance types, specifying storage capacities, and configuring network settings. Provisioning establishes the foundation upon which deployments can be made.



Deployments involve the process of deploying applications or services onto the provisioned infrastructure. It includes tasks such as installing and configuring the necessary software components, setting up dependencies, and ensuring the application or service is ready to run. Deployments focus on making the application or service operational and available for use.

Provisioning

Provisioning includes planning, integrating, and deploying new virtual assets or functionalities. It includes setting up virtual networks, creating new virtual machines, and configuring cloud-based services to meet the specific needs of the agency. Your operating model (see [Selecting an Operating Model](#)) will greatly influence how your agency provisions or deploys cloud assets. There are many potential tools and approaches to conduct this work, and good practices will enable effective provisioning. Typical provisioning areas include:

- **Provisioning Environments.** This includes creating virtual private clouds (VPCs), setting up security groups, configuring access control lists (ACLs), configuring virtual private networks (VPNs), and cloud connect circuit connections.
- **Onboarding Users.** Users in this context would likely include developers and administrators. This process involves guiding new users through the steps required to access cloud resources. It includes setting up user accounts, configuring authentication mechanisms, and providing guidance on how to use the cloud-based services and resources available.

Additional considerations for provisioning include:

- Aligning your provisioning approach with your operating model. For example, a centralized system would likely have a different provisioning approach than a decentralized operating model (e.g., shared accounts vs. hierarchical accounts).
- Establishing a provisioning and deployment policy and process that:
 - Accounts for strategy, need, operating model, resources, financial management, and security
 - Maintains a service catalog
 - Tags newly-provisioned assets
 - Develops and maintains workflows for self-service and automated provisioning.
 - *Self-provisioning* allows users to allocate their own machines.
 - *Automated provisioning* allows the service to add or subtract resources as needed.
- Automating repetitive processes like provisioning. For example, CSPs have tools to set up and govern a multi-account environment that can automate the creation, configuration of accounts, shared services and more. The desired outcome is to streamline tasks, deploy standardized resources, and eliminate human error. *Note that automation is likely not a starting point but a goal. It will take effective process management and technical skills to begin leveraging automation.*

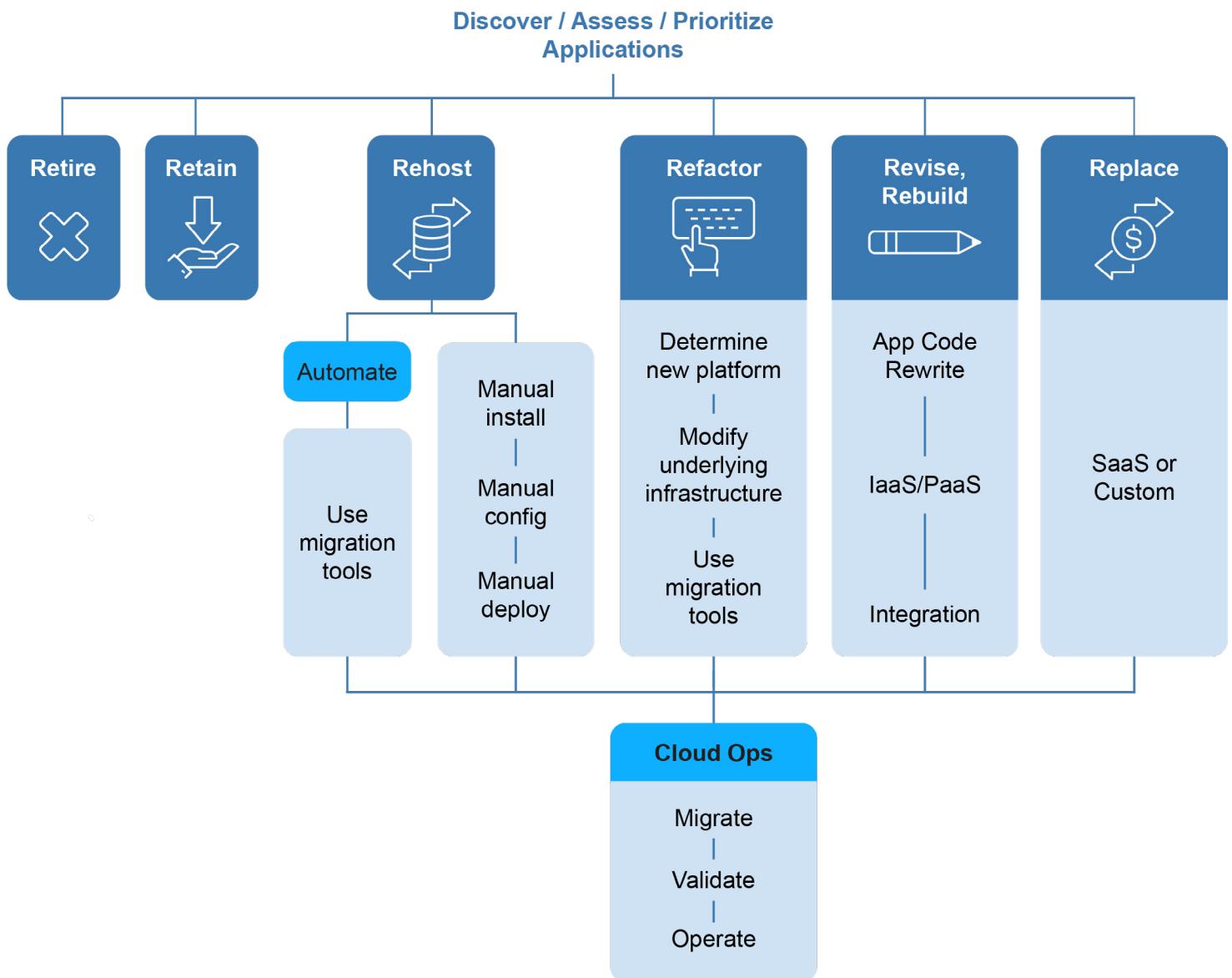


Deployment

Deployments include migrating systems from one environment to another as well as deploying new, cloud-native applications. The tasks for new, cloud-native deployments are a subset of those to be considered for migrations. Therefore, while the focus of this section is on migrations, some of the suggestions are relevant to new, cloud-native applications.

With respect to migrations, an agency has several choices. These are depicted in Figure 17.. More details on these different scenarios are located in [Application Rationalization](#).

Figure 17: Journey Map to Operations Phase, By Planned Disposition





Best practices for migration include:

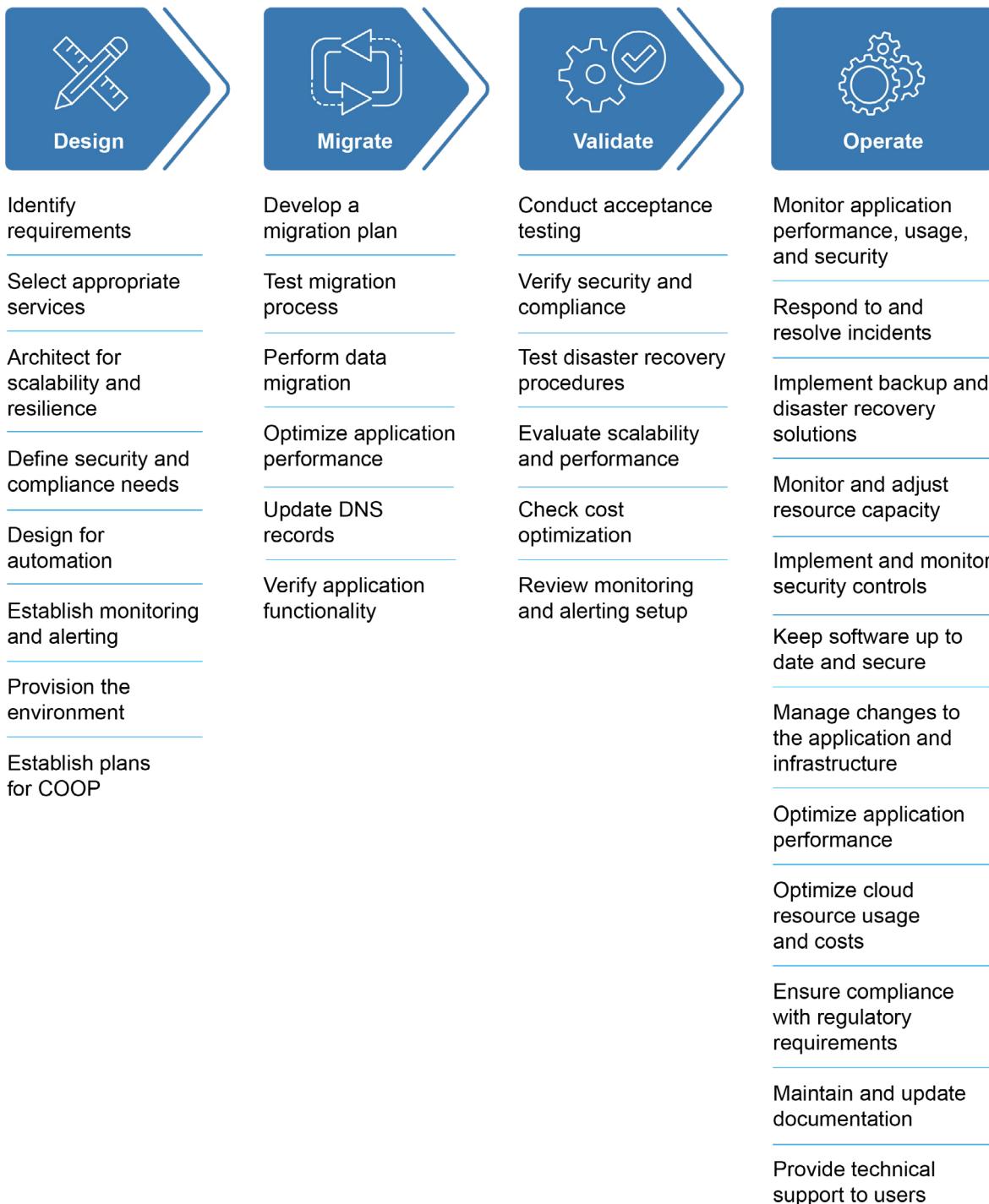
- Check with your CSP to identify available levels or types of migration support (e.g., tools or services)
- Focus on the data
 - Understand the volume and type of data that needs to migrate
 - Understand the expected data flow (volume and type) of the application or service during operations
- Assess the current infrastructure to determine what is to be migrated or not migrated
- Create a migration plan to ensure system integrity, stability, security, and functionality. See the [GSA Application Lifecycle Framework](#) for more details
- Identify the tools and technologies needed for the migration process
- Provision the new environment to ensure it is ready to receive the migrated applications
- Provide post-migration support to ensure the migrated applications run smoothly in the new environment
- Establish checklists, a charter, and the appropriate check-ins to ensure quality, establish expectations, and maintain quality

Figure 18, Typical Migration Tasks by Migration Lifecycle Phase, provides an overview of typical migration tasks that need to be considered. These tasks are organized by the migration lifecycle. Note that this list is typical. The actual steps required may increase or decrease. Use the results of your [application rationalization](#) to determine what is needed.

Regardless of the migration approach, take the time to consider opportunities to leverage cloud capabilities like autoscaling. Even if the application is not cloud-native, there may be low-cost opportunities to implement advanced capabilities. Make this part of both the planning and post-migration review.



Figure 18: Typical Migration Tasks by Migration Lifecycle Phase





Configuration Management

Cloud configuration management is the practice of capturing and managing configuration data for cloud-based resources. It helps ensure cloud resources are properly configured, secured, and optimized for performance. This includes monitoring and managing resource configurations and implementing processes to tag and track resources. Effective configuration management is critical to security. Simply, how do you monitor what you do not know?

Relevant considerations include:

- Automation benefits from standardized resource configurations.
- Multi-cloud or hybrid environments can complicate developing an integrated, enterprise view of configuration data.
- Implement a robust automation framework to manage the configuration of your infrastructure.
- Use a version control system to track and manage changes to your infrastructure configurations. This allows you to roll back changes as needed and eases collaboration.
- Establish and maintain a set of configuration baselines that define the desired state of your infrastructure components.
- Implement a formal change management process to handle configuration modifications.
- Perform regular configuration audits to verify compliance with security standards and established baselines.
- Implement a robust backup and restore mechanism to safeguard your configuration data.
- Deploy comprehensive monitoring solutions to track the performance and health of your infrastructure. Monitor configuration changes, resource utilization, and system logs to detect anomalies and ensure your infrastructure is operating optimally.
- Maintain accurate and up-to-date documentation of your infrastructure configurations.

SUSTAINMENT

Sustainment activities ensure the smooth functioning and longevity of cloud-based systems by focusing on ongoing maintenance, support, and optimization tasks. Key outcomes of sustainment activities in cloud operations include increased system stability, improved performance, optimized costs, enhanced security and compliance, reduced downtime and incidents, efficient resource utilization, and continuous improvement of cloud systems and processes.

Monitoring and Observability

Monitoring and observability are essential practices in cloud operations that help ensure the effective management and troubleshooting of cloud systems. Key task areas include:

- Performance Monitoring
- Problem Detection and Diagnosis



- Capacity Planning
- Incident Response and Recovery
- Optimization and Cost Management

Best practices include:

- Identify the key performance indicators (KPIs) and metrics that align with your system's goals and user requirements. Example metrics include response times, error rates, throughput, and resource utilization.
- Establish real-time monitoring to detect and respond to issues promptly. Leverage monitoring tools that provide alerts and notifications based on defined thresholds or anomalies.
- Implement distributed tracing to gain insights into the end-to-end behavior of complex, microservices-based applications. This helps identify bottlenecks and latency issues across the entire system.
- Aggregate logs from different components and services to gain a comprehensive view of system behavior. Utilize log analysis tools and techniques to extract valuable insights and perform root cause analysis. See also [Logging Management](#).
- Implement auto-scaling capabilities based on predefined metrics to dynamically adjust resources to meet fluctuating demand, ensuring optimal performance and cost efficiency.
- Develop dashboards or visualizations to clearly present data for effective decision making and troubleshooting.

Optimization & Tuning

Optimization and tuning strive to improve performance, cost-effectiveness, support capacity planning, and enhance security measures. While optimization focuses on enhancing overall system performance and resource utilization, tuning involves fine-tuning specific components or configurations to achieve optimal performance.

Best practices include:

- Establish a performance baseline for comparison and evaluation
- Conduct rigorous testing and validation of optimizations and tuning changes in staging or test environments before implementing them in production
- Share expertise, insights, and best practices related to optimization and tuning between development, operations, and infrastructure teams
- Utilize performance profiling tools and benchmarking techniques to identify performance bottlenecks, pinpoint areas for improvement, and analyze the impact of optimization or tuning changes
- Maintain comprehensive documentation
- Continuously optimize resources and environments



- Automate repetitive tasks and creating custom scripts to streamline cloud operations, increase efficiency, and reduce manual errors
- Identify CSP-native tools that support optimization and tuning

Network Considerations

Network considerations for the cloud include implementing security protocols, optimizing network architecture, managing bandwidth and latency, using load balancing strategies, segmenting networks, utilizing monitoring tools, and updating firewall rules. Specific areas include:

- Design and update the network architecture to account for factors such as traffic patterns, application dependencies, and latency requirements
- Define subnet strategies and IP address management practices
- Implement robust network security measures like firewalls, network access control lists (ACLs), and security groups
- Monitor networks like bandwidth and latency

Best practices include:

- Segment networks to improve security and control access to critical systems and data.
- Utilize network monitoring tools to identify and troubleshoot network issues in real time.
- Regularly review and update firewall rules and security groups to ensure proper access controls and limit exposure to security risks.
- Implement DNS resolution for applications to simplify access and management of application endpoints.
- Familiarize yourself with the networking services offered by your cloud provider, such as virtual networks, load balancers, DNS management, and network security groups.
- Utilize VPC or similar concepts provided by your cloud provider to create isolated virtual networks and establish network-level controls and security boundaries.
- Leverage auto-scaling groups and elastic load balancers to handle traffic fluctuations.
- Segregate your network resources based on functional or security requirements using subnets or virtual network segments to control traffic flow and isolate sensitive resources.
- Periodically review and optimize network configurations to ensure they align with your evolving requirements. Remove unused resources, optimize routing, and adjust configurations based on performance monitoring and analysis.
- Estimate and plan network bandwidth requirements based on expected traffic patterns, data transfer, and user demands. Scale up your network bandwidth as needed to ensure optimal performance.
- Utilize private IP address space within your VPC or virtual network to minimize the exposure of your resources to the public internet and enhance security (may not be relevant in zero trust environment).



- Implement load balancing strategies to distribute network traffic efficiently and avoid network congestion (may be typically managed by CSPs). Maintain up-to-date documentation of your network configurations, security policies, and connectivity requirements.

Useful telecommunications resources can be found at GSA's [Enterprise Infrastructure Solutions Resources](#).

IPv6

As mandated by [M-21-07, Completing the Transition to IPv6](#), all federal networks must move to IPv6-only networks. Agencies should prioritize the implementation of IPv6-capable systems as part of any new systems or modernization to support this transition. Agencies are required under the memo to reach 20% IPv6-only networks by the end of FY23 and 80% by the end of FY25.

Cloud and external services are not specifically covered by M-21-07. Regardless, agencies should consider how cloud architecture impacts the IPv6 transition. Exploring IPv6 adoption within cloud environments often enables **faster, cheaper, and easier** experimentation and implementation than traditional on-premise environments. IPv6 exploration in the cloud can leverage benefits such as native environment isolation, on-demand IPv6 provisioning, and resource auto-scaling, to have more immediate control over testing environments and resources.

Best practices include:

- Explore CSP-supported capabilities for IPv6 dual-stack vs. IPv6-only (support varies between cloud providers)
- Develop an IPv6 addressing plan for structuring, assigning, and managing IPv6 address allocations
- Implement subnet allocation strategies that take into consideration CSPs, regions, and individual virtual network counts
- Identify agency requirements for various addressing types (Global Unicast, Unique Local Addressing [ULA], Link-Local)
- Recognize supported transport mechanisms for IPv6 Routing (Cloud VPN Tunnel, Dedicated Connections, Hosted Connections, etc.) and understand any constraints associated with each supported connection type
- Execute all necessary address ownership and verification steps (RADb, RPKI, ROA, Certificate of Ownership)
- Confirm which cloud infrastructure components (Firewalls, Application Load Balancers, Network Load Balancers, etc.) are compatible with the IPv6 services you have chosen to deploy (compatibility varies between cloud platforms and component vendors)
- Avoid usage of Network Address Translation (NAT), where possible, to maximize the benefits of the native IPv6 addressing format

Contact your agency's IPv6 Integrated Project Team (IPT) or Transition Manager to learn more.



Find IPv6-compliant products by visiting the [USGv6-r1 Product Registry](#). This registry is operated by the University of New Hampshire InterOperability Laboratory. Listed products conform to [NIST USGv6 Rev 1](#) standards and have been tested using ISO/IEC 17025 accredited testing.

If you have questions about IPv6 testing or how to test new or unapproved products, contact the [NIST USGv6 program](#). For policy or compliance questions about M-21-07, contact the Federal IPv6 Task Force at dccoi@gsa.gov.

Trusted Internet Connection

The Trusted Internet Connections (TIC) initiative refers to a framework to modernize and enhance network security across federal agencies. TIC aims to enable secure and efficient access to the internet and cloud services while maintaining strong security controls. Designing TIC-compliant networks can be complex, especially when accommodating hybrid or multi-cloud scenarios.

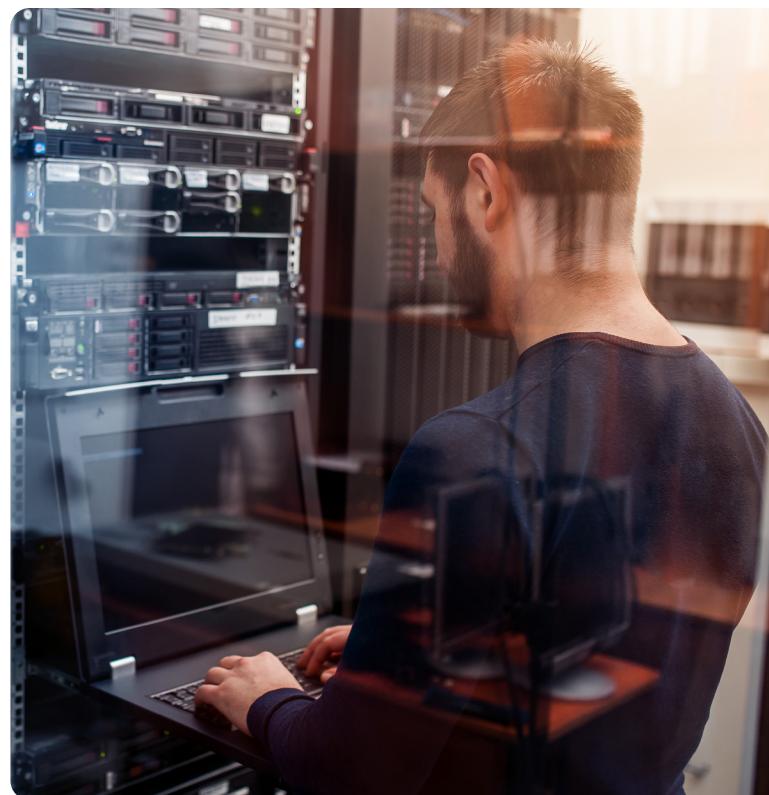
CISA provides authoritative TIC resources for federal agencies:

- [CISA Trusted Internet Connection resource page](#)
- [Trusted Internet Connections 3.0 Core Guidance documents](#) (Program Guidebook, Reference Architecture, Security Capabilities Catalog, Use Case Handbook, Overlay Handbook)

Data Ingress & Egress

The ingress and egress of data can cause significant performance and cost issues. These issues can appear in both migration scenarios as well as typical use. These issues must be addressed to effectively address expectations and budgets.

Relevant performance-related issues include: bandwidth limitation imposed by CSPs; latency as data is transferred between environments; and network congestion. Cost-related issues include: CSP charges for data ingress and egress (especially when transferring data across regions or between different cloud providers); egress charges related to retrieving or downloading data; and data transfer overage charges.





Best practices include:

- Keep the application and data close
- Use data compression techniques, parallelization, and efficient transfer protocols to minimize the volume and time required for data transfer
- Explore options provided by CSPs like data transfer acceleration services or content delivery networks (CDNs) to improve transfer speeds and reduce latency
- Use physical data transfer appliances provided by CSPs for large-scale or initial data transfers
- Monitor data transfer usage to track costs and optimize
- Design cloud-based systems to minimize unnecessary data transfer across regions or providers

Service Management

Service management refers to the management and maintenance of the delivery of cloud services to customers or users. It encompasses various tasks aimed at ensuring the availability, performance, security, and continuous improvement of cloud services, including:

- Planning cloud services to meet customer requirements.
- Provisioning and configuring the necessary components.
- Tracking performance, availability, and compliance with service level agreements.
- Addressing and resolving incidents or problems.
- Managing changes to services and infrastructure.
- Planning and optimizing resources.

Best practices for service management include:

- **Establish Service Level Agreements (SLAs).** SLAs are the foundation of any cloud service management plan. SLAs should clearly define the expectations regarding service availability, response times, and performance levels. Both the provider and the customer should understand and agree on these terms.
- **Conduct Continuous Monitoring.** Continuous monitoring can detect potential issues before they become problems. Utilize real-time monitoring to track the performance of applications and resource utilization.
- **Integrate Incident Management.** Integrate cloud-based issues into the agency's existing incident management processes.



- **Modernize Change and Configuration Management.** Change management setup for traditional on-premise environments may have long lead times. Update your current change and configuration management processes to align with the faster-paced, agile needs of the cloud.
- **Optimize Resources.** Regularly evaluate your resource needs and usage. Plan for future needs based on usage trends and planned initiatives. Analyze your data often to best manage utilization and performance.

Service Resolution

Service resolution identifies, addresses, and resolves issues or incidents that affect the availability, performance, or functionality of cloud-based services. It involves promptly responding to service disruptions, investigating the root causes, and implementing appropriate measures to restore normal service operations. Key tasks include:

- Detecting and logging incidents
- Establishing an incident response plan with roles, responsibilities, and escalation procedures
- Identifying root causes, implementing workarounds or mitigation strategies as needed, and developing resolution plans
- Communicating with stakeholders on status, resolution, and timeframes
 - Monitoring SLAs and ensuring that service performance meets or exceeds agreed upon targets

Best practices for service resolution include:

- Prioritizing incidents and ensuring stakeholders understand assigned priorities
- Fostering collaboration between teams
- Documenting resolutions and addressing root causes
- Leveraging automation

Software Updates and Releases

Software updates and releases refer to the deployment of new versions, patches, or bug fixes to software applications running in the cloud. It ensures software is up to date, secure, and optimally performing. It includes tracking code changes, controlling feature releases, testing in staging environments, automating deployment, using deployment strategies to minimize downtime, and developing rollback and recovery procedures.

A new approach to managing software updates is immutable infrastructure. Immutable infrastructure refers to software or systems that are never modified and remain in the same state. A goal for operations teams should be to adopt an approach that supports immutable environments, where direct changes to production servers and applications are avoided, and any changes are made to a new build and pushed into production. There are many benefits to



this approach, such as preventing configuration drifts, simplified and reliable deployments, consistent testing and debugging environments, safer deployments with easier rollback, and easy scalability with increased security profiles. See the [Containerization Readiness Guide](#) and [M-22-09 Federal Zero Trust Strategy](#) for more information regarding immutable environments and federal requirements to support the Federal Zero Trust Strategy.

Best practices related to software updates and releases include:

- Use a version control system to track code changes.
- Implement controlled release of new features to users.
- Communicate with stakeholders about updates.
- Test updates and releases in a staging environment before deploying to production.
- Use tools to automate the process of deploying software updates and releases across multiple systems, reducing manual effort and ensuring consistency.
- Use blue-green deployment or canary release strategies to minimize downtime and impact on users.
 - **Blue-green deployment** involves having two identical environments, referred to as the blue environment and the green environment. The blue environment represents the production environment where the current version of the software is running. The green environment represents the new version of the software that is being deployed. The deployment process involves the following steps:
 - Initially, all user traffic is routed to the blue environment, ensuring the production environment is stable and functioning correctly.
 - The new version of the software is deployed to the green environment, allowing it to undergo testing and validation.
 - Once the green environment is deemed stable and passes all necessary tests, the router configuration is switched to direct user traffic to the green environment.
 - The blue environment now becomes the inactive environment and can be used as a fallback option if any issues arise during the green environment's deployment.
 - The key benefit of blue-green deployment is that it allows for seamless rollbacks in case any issues are detected in the green environment. If problems arise, the router



Containerization Readiness Guide

May 12, 2021

Office of Information Integrity and Access

General Services Administration
Office of Government-wide Policy



configuration can be switched back to the blue environment, immediately reverting to the previous version of the software without any significant downtime.

- **Canary release** is a deployment strategy that involves gradually rolling out a new version of the software to a subset of users or servers before making it available to the entire user base. This approach allows for controlled testing and validation of the new version in a production-like environment. The deployment process typically follows these steps:
 - A small percentage of users or a specific group of servers is selected to receive the new version of the software.
 - The new version is deployed to the selected users or servers, while the remaining users or servers continue to run the stable version.
 - The behavior and performance of the new version are closely monitored, and feedback is collected from the users or servers in the canary group.
 - Based on the feedback and monitoring results, necessary adjustments and improvements can be made before rolling out the new version to the entire user base or server pool.
- Develop rollback and recovery procedures in case of issues with updates or releases.
- Update configurations and deploying software, includes patch management and operating system support.
- Leverage CI/CD-type software flows to create efficient and effective workflows and operational performance.

Testing

Testing is used in every aspect of the cloud to ensure services are meeting expectations and deployments are providing the expected value without introducing errors. Good testing practices are an integral part of quality management.

Traditional testing is associated with software development but can be adapted to address other types of infrastructure updates or patching activities. Typical forms of testing include:

- Unit Testing: Focuses on testing individual units of code in isolation
- Integration Testing: Verifies the interaction and compatibility between different units of code or components
- System Testing: Expands testing scope to evaluate the behavior and functionality of the entire system as a whole. End-to-end scenarios to validate that different components work together seamlessly.
- Performance Testing: Evaluating system's responsiveness and scalability under anticipated workloads
- Security Testing: Verifying the system is resistant to attacks, assessing data protection mechanisms, and testing for vulnerabilities



Chaos Engineering

A relatively recent innovation is [chaos engineering](#). Chaos engineering involves the deliberate introduction of controlled failures or disruptions to observe how a system behaves and recovers. It helps uncover weaknesses, enhance resilience, and identify areas for improvement.

Obviously, this sort of testing requires careful planning, monitoring, and analysis to avoid impacting customer experiences negatively. Conduct chaos experiments in non-production or isolated environments, and be prepared to respond to any unexpected issues that arise during testing. Start with simpler chaos experiments, such as introducing network latency, component failures, or traffic spikes, and observe the system's response. Gradually increase the complexity and impact of the experiments.

Continuity of Operations

Continuity of operations (COOP), also called disaster recovery, are the strategies and practices used to ensure the availability, resilience, and uninterrupted operation of cloud-based systems and services. COOP or disaster recovery must be built into every cloud-based system. Simply moving to the cloud does not assure an effective recovery. It requires planning and implementing measures to mitigate the impact of disruptions (e.g., cyber-attacks, system failure, and service outages). Key tasks include:

- Establishing business impact to prioritize critical systems and functions.
- Determining mean time to recovery (MTTR), recovery time objectives (RTOs), and recovery point objectives (RPOs).
- Developing plans, policies, process, and roles/responsibilities.
- Implementing regular and automated backup, including frequency, retention periods, and backup storage locations.
- Testing data recovery processes to ensure they are effective and reliable.
- Evaluating service level agreements by cloud service providers.

Best practices include:

- Establish detailed procedures for failovers and recoveries to include roles and responsibilities.
- Periodically test backups and procedures.
 - Implement geographical redundancy by replicating data and applications across multiple data centers or regions to reduce the risk of downtime.
 - Configure automatic failover for critical systems and applications to minimize downtime in case of a failure.

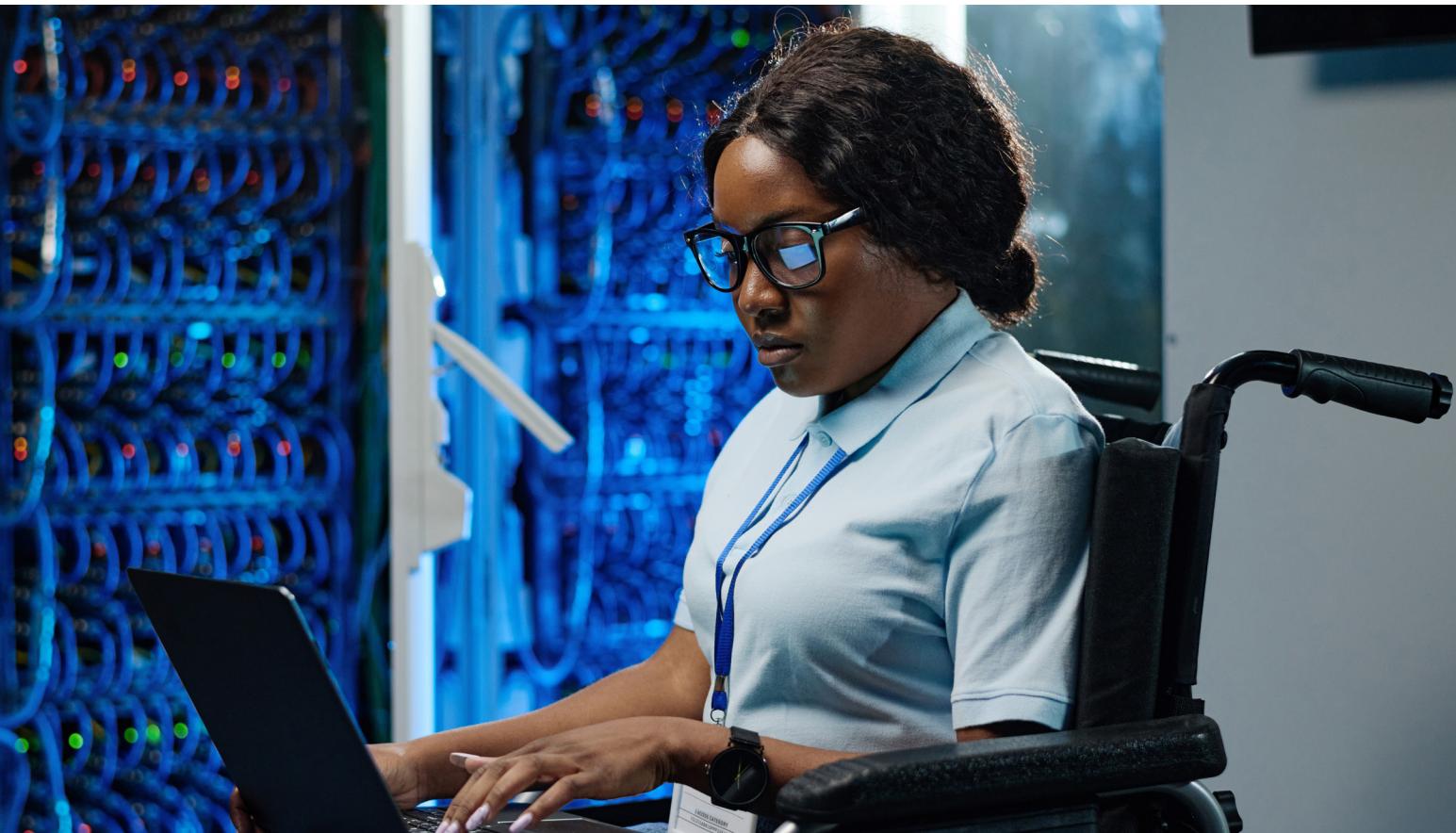


CONCLUSION

In conclusion, this guide describes the best practices for each component of cloud operations. Important takeaways for your agency include:

- **Planning.** Operating in a cloud environment requires extensive planning before an agency can migrate. Considering overall agency strategy as well as available cloud capabilities, agency leaders are encouraged to make informed decisions when it comes to migrating to the cloud.
- **Cloud Strategy.** When it comes to cloud operations, agencies must keep in mind their broader agency IT and Capital Planning Strategy as well as capabilities. Always consider the financial and non-financial costs when making decisions that impact your cloud operations.
- **Agility.** Operating your cloud investment is fundamentally different from traditional on-premise or data center operations. An organizational mindset shift is required to successfully carry out effective cloud operations.
- **Continuous Improvement.** Managing cloud operations requires continuous improvements to create a fully optimized and effective cloud environment. This is true for both technical and non-technical processes.

Call to action: After completion of this guide, conduct a gap analysis of which areas of cloud operations your agency would like to expand. Determine the optimal future state of your cloud operations, the current state of your cloud operations, and the gaps that need to be filled. Use this best practices guide to help your agency determine the necessary steps to fill those gaps.





APPENDIX 1: ASSESSING READINESS FOR CLOUD MIGRATIONS

The following list of questions is used by a large federal agency to determine its readiness to move to the cloud. The insights offer a starting point to manage expectations and resources given a particular agency's readiness. Please note, the list of questions was slightly modified for broader applicability by this document's authors.

Below is a list of eight questions that will help gauge your agency's readiness for migration to the cloud. While many of these questions focus on areas on the periphery to cloud readiness at first glance, without the proper culture, training and "fail fast" mentality, any journey to the cloud will be very difficult. More importantly, the journey may not produce the benefits your agency has identified as priorities.

1. Please rank your agency's priorities when it comes to cloud migration, specifically Infrastructure as a Service (IaaS) cloud services from the list below:
 - a. Cost Savings and Avoidance
 - b. Security
 - c. Performance
 - d. Elasticity
 - e. Disaster Recovery and Availability
 - f. Agility
 - g. Other – Provide priorities not listed above

2. Does your agency have an overall cloud strategy?
 - a. If yes, does it include a multi-cloud component in that strategy?
 - i. If yes, how do you manage your multi-cloud environment?
 - ii. If not, what is the reason you have not considered having a multi-cloud strategy?

3. What metrics and capabilities is your agency considering having for cloud cost management?
 - a. Does your agency plan to conduct regular reviews of the cloud bill with internal teams that generate the cloud costs?
 - b. Does your agency plan on auditing to clean up cloud services to ensure optimal usage and lower costs?
 - c. Does your agency plan to publish the cloud bill for all "consumers" of the cloud services to understand their cloud costs even with a no chargeback model?

4. Does your agency have a mindset that enables it to adopt practices that embrace newer approaches to technical and business processes?

 - a. Does your agency practice the four core values and twelve principles outlined in the Agile Manifesto? (See The Agile Manifesto and 12 Principles of Agile.)
 - b. Is your agency familiar with the Department of Defense guide “Detecting Agile BS” and has it answered the questions presented in this short guide?
 - c. Has your agency started or been using DevOps practices?

 - i. If yes, please describe your CI/CD pipeline at a high level?
5. Are all servers or other hardware devices virtualized with no mainframe or specialized hardware configurations?

 - a. Has your agency prepared an application assessment? Specifically, does your agency have a solid idea on which applications are cloud ready and which applications cannot be migrated easily or migrated at all?

 - i. Any idea on rough order of magnitudes on costs for the applications assessed to move to the cloud?
 - b. Consider network appliances, SANs, network flow devices, etc.
 - c. Does your agency desire to modernize applications with your cloud migration? If yes, how many applications and what percentage of your application portfolio?
 - d. Does your application portfolio have a lot of dependency requiring them to be migrated all at once to avoid key pieces in a hybrid state and possible performance impacts (e.g., Web Front and Database backend)?
6. Does your internal IT group have a collaboration chat tool?

 - a. If yes, please answer below:
 - b. Does everyone from the CIO to the Help Desk technician use this tool to communicate and understand what is going on within the IT organization?

 - i. Does senior IT management have access to many of the collaboration rooms, channels, and sites and use it?
 - ii. Is everyone in IT actively using and communicating with these tools or still using email primarily for internal communications?
7. How many federal and contractor IT staff are certified in the cloud service your agency is using or planning to migrate to?

 - a. For example, with IaaS platforms, involving cloud architects throughout the planning and migration process is very important for making the right call for the many decisions required in this journey

 - i. If you answer 0, then you have a problem.
 - ii. Please describe your existing cloud ecosystem. Specifically, what IaaS, PaaS and SaaS solutions is your agency currently using?

1. NOTE: Your agency may be accessing cloud services through a managed service. Please include those cloud services.
 - I. Example: Accessing a Help Desk ticketing solution that is cloud based via a managed service contract used to acquire Help Desk services.
8. Last question - How many members are in your IT org including contractors and how much money does IT roughly spend each year?
 - a. Generally, the larger the agency (500+), the more challenging culture and communication can be for overall cloud success.



APPENDIX 2: CAPACITY PLANNING TEMPLATE

This template is provided as-is and was created by a federal agency for their use. It should be modified accordingly to meet your agency's particular needs.

Capacity Planning Template

Date: _____ Approver: _____ Tracking Number: _____

Incident number	Incident Date	Affected Application	System/ Server/ Mainframe / Database Name	Current Storage on the Server (GB)	Used Disk Space (GB)	Unused Space/ Free Space (GB)	Burn Rate % per month	Business Impact	Capacity Forecast	Application POC

Reviewed & Cleaned Old/Archived/
Worklogs/Old Job-Data (Y/N): _____

Capacity Operations Input: _____

Growth Rate	Expectation	Recommendation
Peak utilization of the server		
*Service Capacity Management		
Server Health update info: E.g.: End of life etc.		

***Service Capacity Management** — Include the service demand forecast as an assessment of current service levels and performance.



APPENDIX 3: SAMPLE CLOUD RACI CHART

A RACI (Responsible, Accountable, Consulted, and Informed) matrix for cloud operations helps in defining the responsibilities of different roles involved in managing and operating cloud infrastructure and services. Here's an example of how a RACI matrix for cloud operations:

*Tasks/ Roles

Responsible (R):

The individuals or teams responsible for executing the tasks or activities.

Accountable (A):

The person ultimately accountable for the task or activity, ensuring it is completed successfully.

Consulted (C):

Individuals or teams who provide expertise, guidance, or input into the task or activity.

Informed (I):

Individuals or teams who are kept informed about the progress or outcome of the task or activity.

Cloud Infrastructure

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Designing Cloud Infrastructure Architecture													
Implementing Cloud Infrastructure													
Network Configuration & Management													
Create/Update Cloud Templates													

DevSecOps Pipelines & Foundational Infrastructure

Security Measures and Access Controls

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Password Rotation - Application													
Password Rotation - Infrastructure													

Configuration and Change Management

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Change Request Management													
Infrastructure Version Control													
Application Version Control													
Release Management													
Setup & Configure CMDB													

Incident Management

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Application													
Infrastructure													
Security													

Monitoring - Systems Performance & Availability (Establish Monitoring & Alerting)

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Application													
Security													
Infrastructure													

Log Management

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Security Logs													
Infrastructure Logs													
Application Logs													
Transfer Log Data <i>(High to Low Storage Media)</i>													
Log Data Retention Setup & Cleanup Process <i>(Application & Infrastructure)</i>													

Storage and Capacity Management

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Infrastructure													
Application													
Capacity Planning & Scalability													

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Cloud Storage (Setup & Configure)													

Patch Management

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Infrastructure													
Application													
Validation and Testing													

Problem Management

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Problem Detection and Diagnosis (Root Cause Analysis)													

Operations Support Management

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
SOPs (Reviewing/Updating Cloud operations policies & procedures)													
Providing User Support & Training													
Provisioning & Configuring Cloud Computing Resources													

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Optimizing cloud performance and cost													
Backups, Restore, and Disaster Recovery (DR)													
Operations Support <i>(For example: locked accounts, abandon process, and other actions that require administrative actions)</i>													
Government Regulations & Compliances													
Operations Tools Setup													
Infrastructure Tools <i>(Installation & Configuration)</i>													
Application Tools <i>(Installation & Configuration)</i>													
Decommission/ End-of-Lifecycle (EOL) <i>(Application Component)</i>													
Decommission/ EOL <i>(Infrastructure Component)</i>													
Decommission/ EOL <i>(Network Component)</i>													
N-1 Software Upgrade <i>(Application Component)</i>													
N-1 Software Upgrade <i>(Infrastructure Component)</i>													

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
N-1 Software Upgrade (<i>Network Component</i>)													
Setup Data Egress/ Ingress													

Certificate Management

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Digital Certificate (Application)													
Digital Certificate (Infrastructure)													
Digital Certificate (Network)													

Security Management

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Application Hardening													
Infrastructure Hardening													
Database Hardening													
Vulnerability and Malware scanning (<i>SAST and DAST</i>)													
Data privacy and protection (<i>Application & Data Security</i>)													
Data privacy and protection (<i>Network & Infrastructure Security</i>)													
Data privacy and protection (<i>User & Device Security</i>)													
Data Loss Prevention (DLP) Setup													
Zero Trust Arch. (ZTA) Framework Implementation													
Container Security													

Applications Integration & Data Migration

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Integration Connectivity - Infrastructure													
Data Integration - Application													

Access Recertifications

Tasks/ Roles*	Infrastructure Vendor	Application Vendor	Access & Identity Mgmt.	System Owner	Application Owner	ISSO (Application)	ISSO (Infrastructure)	DevSecOps	Cloud Service Provider	IT Operations	Security Operations	Cloud Architect & Engineering	Enterprise Config. Mgmt.
Recertification of all roles and access permissions for Application													
Recertification of all roles and access permissions for Infrastructure													

1. Roles and responsibilities mentioned in the RACI matrix may vary depending on the organization's structure, size, and specific requirements.
2. Customize the matrix to fit your organization's unique cloud operations setup and include relevant roles and tasks. Also, matrix needs to be aligned with the agency's requirements, governance framework, and compliance regulations.
3. Regularly review and update the RACI matrix as roles and responsibilities may evolve over time or with changes in the cloud environment.

[Appendix 3: Sample Cloud RACI Chart](#)



APPENDIX 4: TYPICAL CLOUD ROLES

Cloud Architect

Description	Common Titles	Competencies	OPM Classification
Responsible for understanding available cloud services and how they interoperate. Oversees cloud strategy including cloud adoption, design, management, and monitoring. Designs and manages the enterprise-wide solution for cloud and its interaction with existing legacy applications and data centers.	Cloud Solutions Architect; Solutions Architect; Infrastructure Architect; IT Architect; Cloud Enterprise Architect	<ul style="list-style-type: none">• Requirements Analysis• Cloud Architecting• Strategic Planning• Solution Architecting	GS-2210 IT Specialist (ENTARCH)

Cloud Finance and License Analyst/Expert

Description	Common Titles	Competencies for Consideration	Existing OPM Classification Alignment
Providing pricing models, pricing analysis, and assists the agency in optimizing its cloud solutions and budget. Works directly with engineers, architects, and administrators to provide up-to-date financial information and help craft agency solutions and updates that align with existing budgets.	Budget Specialist; Financial / Management Analyst	<ul style="list-style-type: none">• Financial Modeling• Pricing Analysis• Cloud Architecting• Cloud Engineering	N/A (Non-IT)

Cloud Operations Engineer

Description	Common Titles	Competencies for Consideration	Existing OPM Classification Alignment
<p>Designs, plans, and implements expertise for cloud-based software. Deploys infrastructure and platform services, manages continuous deployment efforts, and works with software developers to deploy applications and systems. May work with IaaS, SaaS, and PaaS vendors and solutions to deploy solutions for the cloud. Performs analysis on system needs and collaborates with data center-based engineers to deploy public and private clouds.</p>	<p>Operations Engineer; Cloud Engineer; DevOps Engineer; Systems Engineer</p>	<ul style="list-style-type: none"> • Requirements Analysis • Cloud Engineering • Application Development and Deployment • Infrastructure Engineering 	<ul style="list-style-type: none"> • GS-2210 IT Specialist (OS) • GS-0854 Computer Engineering Series

Cloud Security Engineer

Description	Common Titles	Competencies for Consideration	Existing OPM Classification Alignment
<p>Designs, builds, and deploys a security framework and systems for a cloud environment. Provides enterprise-level security and works closely with enterprise architects to assess and test the security of existing applications and software. Works with cloud vendors to build a shared responsibility model of security with the agency and existing vendor services and resources. Provides risk-based assessments and testing for existing environments, and is responsible for ensuring compliance with any regulations and requirements.</p>	<p>Cybersecurity Cloud Specialist; Cloud Security Professional</p>	<ul style="list-style-type: none"> • Cybersecurity • Cloud Architecting • Risk Assessment and Analysis • Security Compliance • Identity and Access Management • Software Development 	<p>GS-2210 Cybersecurity IT Specialist</p>

Site Reliability Engineer

Description	Common Titles	Competencies for Consideration	Existing OPM Classification Alignment
<p>Ensures the smooth and reliable operation of a company's software systems and infrastructure. Bridges the gap between development and operations teams. Focuses on scalable, secure, and efficient systems. Designs, builds, and maintains robust systems that can handle high traffic and deliver optimal performance. Includes monitoring, incident response, automation, and continuous improvement to enhance system reliability.</p>	<p>Site Reliability Engineer (SRE); DevOps Engineer; Systems Engineer; Infrastructure Engineer; Reliability Engineer; Site Operations Engineer</p>	<ul style="list-style-type: none"> • Software Engineering • Systems Administration • Automation and Scripting • Scalability and Performance • Security • Continuous Improvement • Cloud Technologies 	<ul style="list-style-type: none"> • IT Specialist (GS-2210-11/12/13): Entry to mid-level SRE positions. • IT Specialist (GS-2210-14/15): Senior-level or management SRE positions.



APPENDIX 5: CHANGE MANAGEMENT PROCESS AND QUESTIONS TO SUPPORT CYBER-SUPPLY CHAIN RISK MANAGEMENT

1. Consider the cybersecurity risks presented by the specific products and services being procured. For example:
 - a. Consider how the products and services will support the agency's mission and whether use of the products and services is critical to the agency's mission success.
 - b. Consider how the products and services will be integrated into existing agency systems and what risks this poses to those systems.
 - c. Consider whether the products and services will handle information requiring additional controls (e.g., controlled unclassified information [CUI] including personally-identifiable information [PII], classified information).
2. Consider the cybersecurity risks presented by the supply chain supporting delivery of the products and services being procured by, for example:
 - a. Assessing risk by conducting online research on potential offerors or existing contractors, authors, products, application.
 - b. Checking vendor and product status within FedRAMP, federal marketplace, or industry certifications (e.g., SOC2).
 - c. Conducting market research and checking SAM.gov to ensure compliant suppliers exist to provide the specific products and services being procured.
3. Standard Research Categories include:
 - a. The Product (description and purpose)
 - b. The Company (history, ownership, headquarters information, location)
 - c. Customers (names and locations)
 - d. Resellers (names and locations)
 - e. Company, product or customer associations
 - f. Particular attention is paid to product, company, customer, and reseller affiliations with foreign entities.