# FAA Cloud Computing Strategy

**Final - Version 1.0**

**May 2012**

**Federal Aviation Administration**

800 Independence Avenue, SW

Washington, D.C. 20591

## SIGNATURE PAGE

S COOPER 3 MAY 2012

Steven Cooper, Acting Chief Information Officer Date

Pat McNall 5/3/2012

Pat McNall, Acquisition Executive and Chief Acquisition Officer Date

# Table of Contents

## DOCUMENT CHANGE HISTORY

| Version | Date | Description of Changes |
|---|---|---|
| 1.0 | 5/2/2012 | First final version |

# 1. Executive Summary

Cloud computing provides a new way of acquiring and delivering computing resources (infrastructure, platform and software). The adoption of cloud computing presents a compelling opportunity to Federal Aviation Administration (FAA) leadership to address critical IT issues including increased cost efficiency, provisioning speed, flexibility and scalability. Cloud computing offers the potential to bring multiple benefits to the FAA due to economies of scale, commoditization of IT infrastructure, and a pay-per-use model. In addition, there are potential cloud computing benefits that can support and accelerate existing Federal and FAA IT initiatives including data center consolidation, net-centric operations, information sharing, shared services, innovation, and sustainability.

While the adoption of cloud computing offers multiple potential benefits to the FAA, it also presents critical challenges and risks that must be considered when evaluating and deciding to use cloud computing. Depending on the mission, goals, and characteristics of individual FAA IT programs, the adoption of cloud computing may introduce levels of risk that are not acceptable when balanced against the performance, safety, security, and reliability requirements associated with air traffic management and control systems .

To accelerate the adoption of cloud computing across the government, the Office of Management and Budget (OMB) made cloud computing an integral part of the *25 Point Plan to Reform Federal Information Technology Management*[1]. As part of the plan, OMB instituted a “Cloud First” policy. This policy requires agencies to consider and evaluate a safe and secure cloud computing option before making new investments. If such an option exists, then OMB is expecting that agencies consider this as the default option. The purpose of this document is to define an actionable strategy to capture cloud computing benefits across the FAA, while continuing to maintain a safe, secure and reliable environment for air traffic management and control systems that enable and support FAA’s mission. The scope of this strategy is FAA-wide including National Airspace Systems (NAS) and non-NAS, wherever cloud computing is applicable.

The FAA’s Cloud Computing vision is the following:

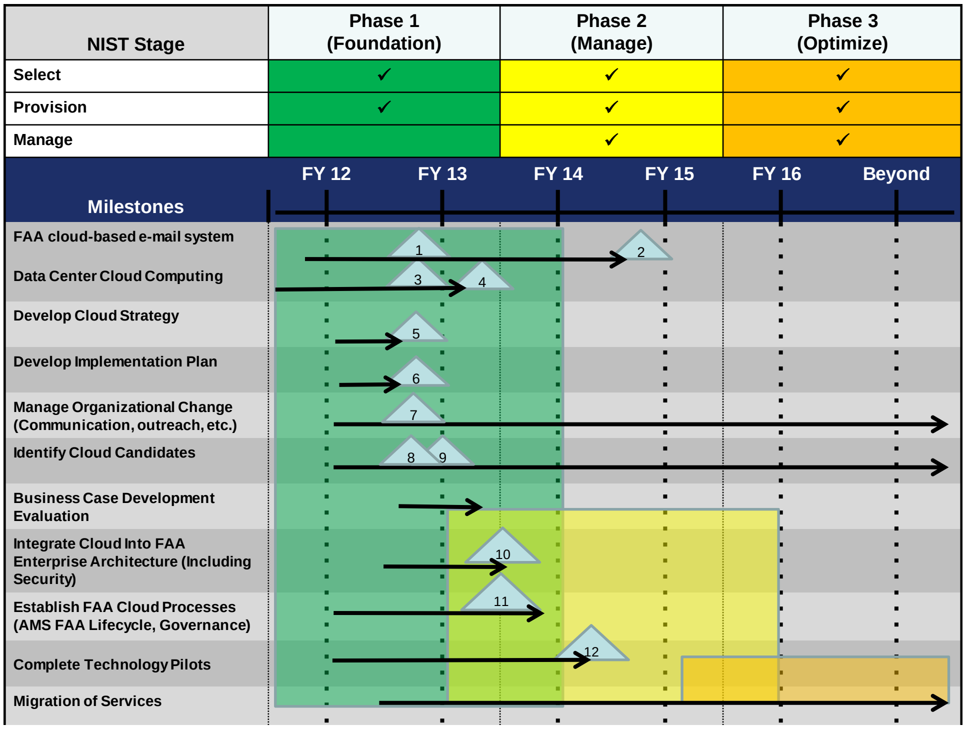
> *Identify and migrate suitable IT services to a cloud computing environment to reduce costs and increase IT provisioning speed, while ensuring that FAA Air Traffic Control and Management systems maintain their current high levels of safety, security, reliability, and performance.*

To achieve this vision, the FAA has identified the following goals:

[1] OMB, 25 Point Plan to Reform Federal Information Technology Management, December 9, 2010, http://www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf

- GOAL 1: Adopt a FAA-wide approach to cloud computing. The FAA will define and adopt a comprehensive approach to identify, evaluate, select, migrate, and operate cloud services.
- GOAL 2: Define and develop an FAA Cloud Computing Architecture and integrate it into the FAA's Enterprise Architecture (EA). The FAA EA will be expanded to incorporate cloud computing architectural elements as required.
- GOAL 3: Develop a cloud computing program implementation strategy. The FAA will ensure that all relevant processes and policies support cloud computing program adoption as required.
- GOAL 4: Increase the efficiency of current and future IT investments. Ensure that potential benefits are captured and measured along the FAA lifecycle.
- GOAL 5: Manage technical and management risks and support FAA transition to cloud services. Manage risks, and comply with external and internal mandates and regulations.

This strategy uses a risk-based incremental approach, and it has initially identified three phases for the adoption and migration of cloud services: 1. Foundation (establish the initial capability); 2. Manage (mature practices and technologies); and 3. Optimize (move higher risk operations to cloud).  Figure 1 summarizes the high level roadmap for the FAA Cloud Computing Strategy. The scope and number of phases may be adjusted in the future to reflect Federal and FAA priorities and funding levels.



| NIST Stage | Phase 1 (Foundation) | Phase 2 (Manage) | Phase 3 (Optimize) |
|---|---|---|---|
| Select | ✓ | ✓ | ✓ |
| Provision | ✓ | ✓ | ✓ |
| Manage |  | ✓ | ✓ |

**Figure 1. FAA Cloud Computing Strategy Roadmap**

NAS and non-NAS systems have different imperatives, objectives, and characteristics and they are represented by two different enterprise architectures. Given these differences, at a tactical level, the FAA will need two different implementation and execution strategies that are aligned with the overall direction of this unified FAA Cloud Computing Strategy, and they will address different criticality and sensitivity levels of NAS and non-NAS systems.

In support of OMB's "Cloud First" policy and the Federal Cloud Computing Strategy, FAA has already initiated a few existing cloud computing initiatives. The FAA Cloud Computing Strategy will advance and accelerate the current adoption of cloud computing across the FAA to capture benefits and provide tangible business value, while ensuring that air traffic management and control systems are safe, secure and reliable in support of FAA's mission. To achieve this, the FAA will use an structured engineering approach to balance requirements, schedule, cost and risk when deploying cloud technology.

# 2. Introduction

In 2010, OMB published the *25 Point Implementation Plan to Reform Federal Information Technology Management*[2]. The 25 Point IT Plan attempts to clear obstacles to adopt IT best practices, allowing the Federal Government to leverage information technology to create a more efficient and effective government. Cloud computing is an integral part of the 25 Point IT Plan. In 2011, OMB also published the *Federal Cloud Computing Strategy*[3], which articulates the benefits, considerations, and trade-offs of cloud computing, provides a decision framework and case examples to support agencies in migrating towards cloud computing, highlights cloud computing implementation resources, and identifies Federal Government activities, roles, and responsibilities for catalyzing cloud adoption. Furthermore, OMB instituted a “Cloud First” policy. This policy requires agencies to consider and evaluate a safe and secure cloud computing option before making new investments. If such an option exists, then agencies must use the cloud solution as the default. The FAA needs an overarching strategy to accelerate the adoption of cloud computing across the Agency and capture its potential benefits, while ensuring that air traffic management and control systems remain safe, secure and reliable to fulfill FAA’s mission.

## Purpose and Scope

The purpose of this document is to define and communicate a unified FAA’s direction and strategy on cloud computing. It is also intended to serve as a communication vehicle within the Agency and with external organizations as required. It is not intended to define, prescribe or constraint any particular technical approach, plan or solution, service type, or deployment model.

The scope of this document is FAA-wide including NAS and non-NAS systems wherever cloud computing is applicable. NAS and non-NAS systems have different imperatives, objectives, and characteristics and they are represented by two different enterprise architectures. The NAS is characterized by real-time and safety-critical operations, a mixture of Internet Protocol (IP) and non-IP systems, and it operates on a closed NAS Federal Telecommunications Infrastructure (FTI) network. The non-NAS supports NAS Programs’ Regulatory and FAA Administrative functions, it is characterized by non-safety critical support functions, and it operates on the FTI Mission Support Network. Given these differences, at a tactical level, the FAA will need two different implementation and execution strategies aligned with this unified FAA Cloud Computing Strategy, and they will address different criticality and sensitivity levels of NAS and non-NAS systems.

[2] OMB, 25 Point Plan to Reform Federal Information Technology Management, December 9, 2010, http://www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf

[3] OMB, Federal Cloud Computing Strategy, February 8, 2011, http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf

## Audience

The intended audience of this document is FAA’s senior leaders and managers, system planners, program managers, technologists, and others responsible for cloud computing adoption.

# 3. Cloud Computing Benefits

The cloud computing business model to deliver IT services (software, platform and infrastructure) presents a compelling opportunity to FAA leadership to address critical IT issues including increased cost efficiency, provisioning speed, flexibility and scalability. Furthermore, there are additional potential benefits from cloud computing that can support and accelerate existing Federal and FAA IT initiatives including data center consolidation, net-centric operations and information sharing, shared services, innovation and sustainability. Given the potential benefits from cloud computing, as part of the execution of this strategy, the FAA will analyze and identify opportunities to take advantage and capture cloud computing benefits across the Agency. Potential benefits from cloud computing are described below.

## Increased Cost Efficiency

A major potential benefit from cloud computing is IT cost savings. Under the cloud computing model, the costs of acquiring, maintaining and refreshing software, tools, development platforms, hardware, storage, etc. are shifted to the cloud service providers (CSPs). CSPs can serve a high number of customers and they are able to offer lower individual pay-per-use rates by leveraging economies of scale, commoditizing infrastructure, and automating data center processes. In a typical IT organization, operation costs represent a significant percentage of the IT budget, and the opportunity to optimize and reduce operation costs by using cloud services represent a very attractive option to IT organizations and the FAA. For instance, many organizations across the FAA maintain multiple servers (hardware and software) with similar characteristics and possibly low utilization rates. Costs that are associated with the servers include the initial acquisition of hardware and software, annual license fees, periodic technology refreshes, and the associated administration and maintenance of the environment. Depending on the criticality and sensitivity of the data and systems that they support, the next time that a group of servers requires a technology refresh, the need for these servers may be provisioned by a CSP in the form of Infrastructure as a Service (IaaS). FAA organizations will then replace typical costs associated with the operations and maintenance of the servers with a lower pay-per-use rate for the servers.

## Increased Provisioning Speed

Another typical pain point in IT is the provisioning speed. Providing new applications, setting up technical environments, developing new software, etc. may take a long time and it is usually not aligned with changing business needs and customer expectations. A key characteristic of cloud computing is the automated provisioning of computing resources and it has the potential to increase dramatically the provisioning speed. For instance, think of a potential scenario where the need for a data and financial analysis tool is presented. The required functionality is already provided in the form of Software as a Service (SaaS) by an authorized CSP. Authorized users in the business and financial teams may get almost immediate access to the SaaS capability on a pay-per-use model. There would not be a need to procure and buy a server, software, connect it to the network, and provide access, before users can use the functionality.

### Scalability

To take advantage of economies of scale, CSP data centers have massive amounts of computing resources available automatically to cloud service consumers. Individual program needs for computing resources may vary for several reasons. An unexpected event, new policies or regulations may trigger increased demand for computing resources that was not forecasted in advance. Cloud computing offers the potential benefit to both scale up and down computing resources as needed. For instance, an unexpected national aviation event can quickly multiply the demand for access to files in the FAA Web site including video and audio. Depending on demand, a traditional IT system will be overwhelmed and eventually fail, where a cloud service will allow to rapidly scale up to meet the unpredictable demand.

### Additional Potential Benefits

Typical benefits from cloud computing have been centered on IT cost savings, increased provisioning speed, and scalability. There are additional potential benefits that are important to existing Federal and FAA initiatives including data center consolidation, net-centricity, information sharing, shared services, innovation and sustainability. Cloud computing can accelerate data center consolidation efforts by reducing and simplifying the existing FAA data centers, which will decrease data center consolidation and integration costs in the future. CSP data centers can be seen as massive repositories of data, applications and computing resources accessed via a network with the potential for interconnectivity that creates a network of networks and accelerate net-centric operations and information sharing across the FAA. A network of networks that creates a cloud computing platform will make it easier to share services with authorized internal and external FAA organizations. The affordable and quick access to massive cloud computing capabilities can be seen as a lab in the desktop that may spur innovation across the FAA. The elimination of redundancies and optimal utilization levels in the FAA IT environment will reduce energy consumption and support a more sustainable environment.

# *4. FAA Cloud Computing Vision and Goals*

The FAA's Cloud Computing vision is to:

> *Identify and migrate suitable IT services to a cloud computing environment to reduce costs and increase IT provisioning speed, while ensuring that FAA Air Traffic Control and Management systems maintain their current high levels of safety, security, reliability, and performance.*

The FAA envisions an IT environment that takes advantage of available cloud services (such as infrastructure, platform, software) and deployment models (such as public, private, community, hybrid). The FAA is planning for an IT environment supported by policies and processes across the FAA life cycle that enable the acquisition, creation and consumption of cloud services across the Agency. In the future, most IT initiatives will not require a significant upfront investment, making it easier for the agency to launch strategic IT initiatives. FAA IT organizations will be able to provision services to customers that satisfy FAA's operational demands for flexibility, scalability and timeliness. FAA IT programs will be able to deploy development and test environments quickly and with minimal upfront investments. FAA IT users will be able to access authorized data and services from virtually anywhere, anytime they can establish a secure network connection. IT complexity will be significantly reduced and the IT environment will be adequately protected from growing and evolving cyber security threats. The FAA envisions an IT environment that takes advantage of cloud computing to support, enable or leverage key Federal and FAA initiatives including data center consolidation, net-centric operations, shared services, Service-oriented Architecture (SOA), innovation, and sustainability. The FAA IT environment will be scalable and flexible to take advantage of newer and emerging technologies as required including wireless and mobile computing, data analytics, and social networks. Figure 2 provides a notional depiction of the FAA Cloud Computing Vision.

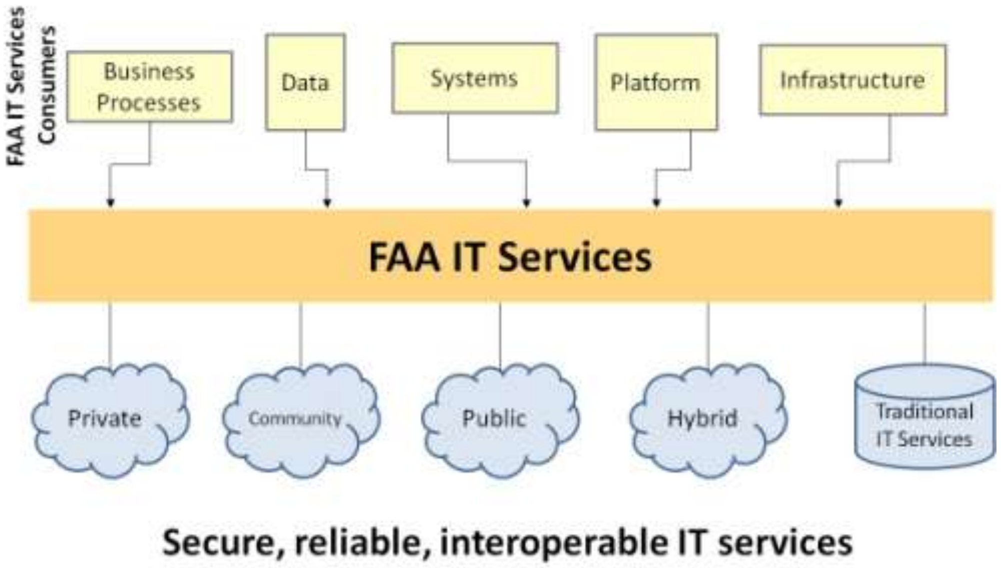


**Figure 2. FAA Cloud Computing Vision**

FAA's cloud computing vision describes the desired state in the future. There are valid concerns with public clouds in some areas of the FAA today, especially related to security and performance requirements. As the technology matures, it is expected that these challenges will be resolved in whole or in part.. To achieve the vision, the FAA has identified five (5) goals. Figure 3 shows the goals that are required to enable FAA's Cloud Computing Vision.

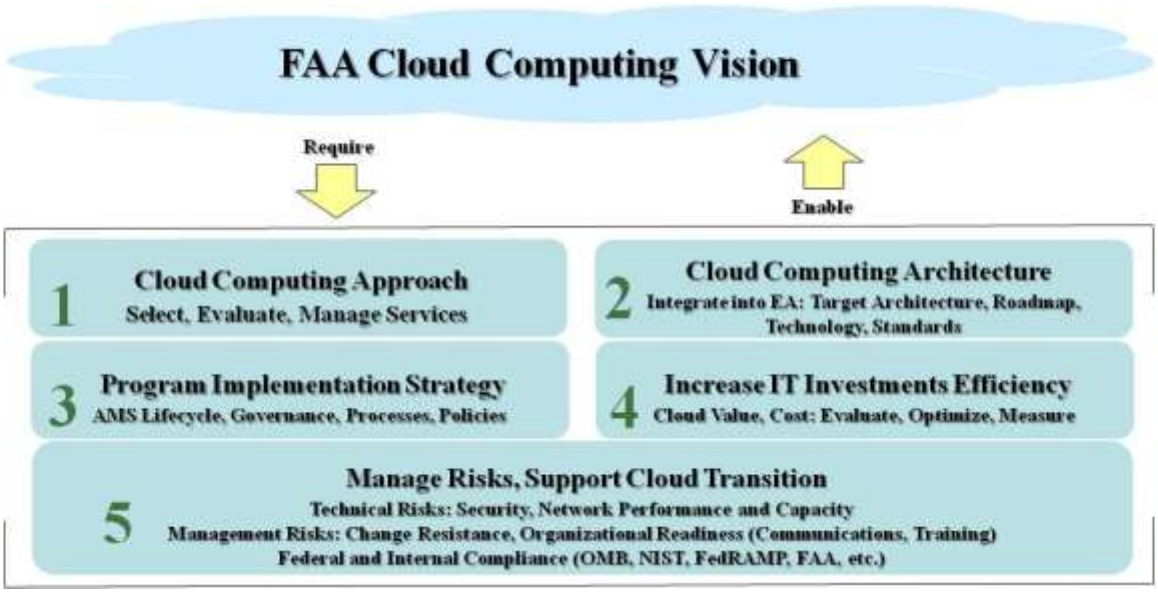

FAA Cloud Computing Vision
Require
Enable
1
Cloud Computing Approach
Select, Evaluate, Manage Services
2
Cloud Computing Architecture
Integrate into EA: Target Architecture, Roadmap, Technology, Standards
3
Program Implementation Strategy
AMS Lifecycle, Governance, Processes, Policies
4
Increase IT Investments Efficiency
Cloud Value, Cost: Evaluate, Optimize, Measure
5
Manage Risks, Support Cloud Transition
Technical Risks: Security, Network Performance and Capacity
Management Risks: Change Resistance, Organizational Readiness (Communications, Training)
Federal and Internal Compliance (OMB, NIST, FedRAMP, FAA, etc.)

**Figure 3 – FAA Cloud Computing Strategy Goals**

The goals to enable FAA's Cloud Computing Vision are described below. It is important to note that while this strategy provides a unique FAA's Cloud Computing Vision and Goals, at the tactical level, specific technical approaches and activities to achieve vision and goals will differ between the NAS and non-NAS domains given their different requirements, objectives, and characteristics.

## GOAL 1: Adopt an FAA-wide approach to cloud computing

The FAA will define and adopt a comprehensive approach to migrate IT services to the cloud. The assessment and selection of FAA IT services that can be migrated to cloud services is the first step. It will be followed by a decision process to determine the cloud service type and the cloud deployment model that best balance cost, value and risk to FAA's mission. Objectives include:

- Perform a comprehensive and holistic analysis of the FAA IT environment to identify candidates for cloud adoption based on benefits and risks to the FAA. This will be an enterprise-level FAA analysis where all relevant FAA programs, business units, and service providers are analyzed for consolidation and optimization opportunities from cloud adoption. The enterprise-level and holistic analysis is key. Typically, FAA studies and analysis are conducted at the program, project or business unit level. To capture cloud computing benefits, the FAA needs to cross program and organizational boundaries to eliminate redundancies and reduce costs. In addition, all components and environments of the architecture need to be evaluated for potential benefits from infrastructure, platform and software services.

- Prioritize candidates for cloud migration. Based on FAA benefits and risks, identified candidates will be quantitatively ranked to provide FAA decision makers with a quantitative and objective priority of the identified candidates. High value and benefits to the FAA will increase the priority score, while high risk will be considered a negative factor for the score. It is expected that non-NAS, and NAS regulatory systems may be earlier candidates for cloud migration, whereas NAS systems may require further and deeper engineering analysis due to their strict security, safety, reliability and performance requirements.
- Develop a business case to measure value and benefits from cloud candidates. Factors that need to be considered for cloud computing include opportunities for consolidation and optimization, elimination of redundancies, economies of scale, and a pay-per-use cost model. IT operations costs to buy, maintain and refresh required software, tools and infrastructure may be significantly reduced or eliminated. In a cloud computing service model, the cloud service provider (internal or external) is responsible for buying, maintaining and refreshing the required IT components. FAA programs as cloud service consumers can use a flexible utility-type pay-per-use model to pay only for IT services that they need and consume without the expenses required for IT components purchase, maintenance and refresh. Specific organizational factors will also be considered. For instance, an existing long term contract may prevent the realization of planned cost savings.
- Identify the cloud deployment model to use (public, private, community, hybrid). The functional performance requirements for each community of information may require that more than one cloud model be used. Based on benefits and risks to the FAA, a recommendation for deployment in the cloud will be made for the identified cloud candidates. Again, the analysis will be based on value and risks to the agency.

### GOAL 2: Define and develop an FAA Cloud Computing Architecture and integrate it into the FAA Enterprise Architecture (EA)

Migration to cloud services will require changes to many dimensions of the FAA and cooperation across the organization. The FAA's EA will ensure that the FAA evolution to cloud services achieves the planned benefits while minimizing risks to ongoing FAA operations. The FAA EA has three components: the NAS architecture, the NAS regulatory architecture, and the non-NAS architecture. Each component of the architecture has different objectives, characteristics and requirements and will evolve differently as required to incorporate cloud elements. In accordance with EA practices, the target architecture to integrate FAA cloud services will be developed. The definition and development of the technology architecture will require an analysis and evaluation of the cloud services technology and vendor market landscape. Technical standards to ensure interoperable cloud services across the FAA will be identified, adopted, and incorporated to the FAA EA. FAA EA artifacts that incorporate and integrate cloud services will be developed to communicate cloud capabilities with NextGen and FAA programs. A key component of the EA will be the definition of metrics to enable the FAA to measure benefits from cloud computing. Objectives include:

- Define and develop the FAA cloud computing reference architecture. Ensure that all cloud computing architectural elements are identified to satisfy, support and enable the cloud migration process.
- Analyze, evaluate and assess the technology and vendor market landscape for cloud computing. The technology and vendor offers are numerous and evolving. Newer and innovative solutions may be offered by relatively small vendors and the FAA will evaluate risks accordingly. There are also government agencies providing cloud services that will be analyzed and evaluated, as well.
- Define FAA cloud computing architectural requirements and develop the target architecture. The target architecture will incorporate the cloud services and deployment models that have been identified by the FAA. The target architecture will consider an enterprise-level approach where the holistic, cross-organizational, cross-program analysis is reflected to capture cloud benefits by eliminating redundancies and reducing costs. The target architecture will serve as a key instrument to communicate and coordinate cloud capabilities with NextGen and FAA programs. The target architecture will identify and address the functional performance requirements of the individual communities of information.
- Identify and adopt cloud computing technical standards. The FAA will collaborate with relevant organizations to identify and adopt technical standards for cloud computing to ensure interoperability. Technical standards for cloud computing are still evolving, but the FAA will need to identify standards that avoid vendor lock-in, while supporting portability and interoperability requirements.

### GOAL 3: Develop a cloud computing program implementation strategy

Processes including IT Governance will be revised to enable the implementation of cloud computing programs and services across the FAA. Processes that support all phases and decision points of the FAA’s Acquisition Management System (AMS) Lifecycle Management Process will be reviewed to identify required changes to incorporate cloud service elements and provide guidance in acquisition and development of cloud computing capabilities. To break silos and promote shared services, the focus will shift from the typical vertical program-based analysis to an enterprise approach with horizontal integration across organizations, programs, and functional areas where cloud computing may provide increased efficiencies. A Cloud Computing Governance model relevant to FAA Programs’ strategy, planning, development and operational phases will be developed to support FAA programs that will acquire and consume cloud services. The existing IT Governance model will be leveraged and re-used to the extent practical. New practices and processes will be developed to guide and support FAA programs and organizations in the selection and implementation of cloud services. Modifications to existing or the creation of new policies will be required to define an actionable strategy that supports and enables cloud services by the FAA. To support OMB's "Cloud First" policy, the FAA will establish its own cloud computing policy to provide guidance to all organizations to evaluate cloud computing capabilities as one alternative in assessing information technology investments. The FAA's Office of the Chief Information Officer (OCIO) will prepare and publish FAA-wide policies to support the "Cloud First" policy. Objectives include:

- As required, revise processes that support all phases and decision points of the FAA's AMS Lifecycle Management Process to incorporate cloud services and align with the Federal Cloud Computing Strategy. Each phase of the AMS Lifecycle Management Process will be reviewed and analyzed to ensure alignment with Federal strategy and to enable the acquisition and development of cloud services by the FAA.
- Revise the existing FAA IT Governance model and develop a Cloud Computing Governance model relevant to FAA Programs' strategy, planning, development and operations to support programs that will acquire and consume cloud services. Compliance with EA will be revised to incorporate adherence to a future target state that incorporates cloud computing elements.
- Revise relevant systems engineering processes across the FAA lifecycle to ensure that they support and enable the adoption and migration to cloud services.
- Identify and review all relevant policies across the FAA lifecycle to ensure alignment and support of Federal strategy and cloud services.
- Develop guidance for programs adopting and migrating to cloud services.
- Define and publish FAA-wide policy to guide all programs and organizations regarding the use of cloud computing capabilities. Policies and guidance will be established for all phases of the FAA's AMS Lifecycle Management Process, as appropriate. The FAA plans to issue the first policy in Spring 2012 to support OMB's "Cloud First" policy and prevent future purchases of computing resources that do not first consider and evaluate the use of cloud computing services.

**GOAL 4: Increase the efficiency of current and future IT investments**

A key benefit of cloud computing is the increased efficiency of IT including the reduction of costs and the rapid provisioning of services, and the FAA must ensure that it is able to capture this key benefit. The analysis and oversight of FAA IT investments will be augmented to evaluate the efficiency and business value of programs implementing cloud services. The FAA will ensure that the value proposition and cost benefits from cloud service investments are realizable and met. The FAA will identify, develop, and monitor performance metrics for cloud service solutions. Objectives include:

- Revise activities within investment analysis phases as required incorporating specific cloud service elements. The FAA will take three specific actions: first, it will assess each current IT investment for its suitability to use cloud computing (this work has already begun, for the 14 programs initially identified by OMB). This assessment will provide the strategic context by which individual program assessments will be validated during the investment cycle. Second, the FAA will review the analytical products produced during the Concepts and Requirements Definition (CRD) phase of the AMS lifecycle at the Investment Analysis Readiness Decision (IARD) of all programs. At this review, the FAA will identify opportunities to guide these programs toward use of common strategies that will result in their ability to use shared IT services – potentially to be offered by a cloud computing capability (if applicable). For existing programs that are conducting investments on additional useful segments this review will be a revalidation and more detailed analysis of the original assessment. By identifying these programs at the IARD milestone, the FAA can direct programs to incorporate specific cloud computing practices in one or more of the three alternatives required at the Initial Investment Decision (IID) AMS milestone (In accordance with OMB's "Cloud First" policy, the FAA is in the process of implementing a directive for all programs entering the CRD phase, that the three required alternatives must use cloud computing whenever a safe, secure and reliable cloud option that meets performance requirements exists. Also, the FAA Joint Resources Council (JRC) checklist has been modified to include cloud computing. If cloud computing is applicable after CRD Readiness (CRDR), then one or more of the alternatives that should be presented at the next AMS milestone would include the use of cloud computing). Finally, the FAA will investigate in-place IT operations in its mission assets for potential migration to cloud computing. This includes testing currently performed at the FAA's William J. Hughes Technical Center (WJHTC), second level maintenance performed at the Mike Monroney Aeronautical Center (MMAC), and training performed at the MMAC (this analysis has begun).

- Develop a performance evaluation framework to evaluate and monitor cloud service investments. At each relevant milestone, decision or check point, the FAA will be able to objectively and quantitatively measure cloud computing benefits from IT investments and compare against target and planned benefits.

### GOAL 5: Manage technical and management risks and support FAA transition to cloud services

Cloud computing is at a relatively early stage of development: it is complex and it is still evolving. Consequently, there are significant technical and management risks and challenges that the FAA must manage.

Cyber security is a key risk and potential obstacle to cloud adoption. The FAA will prepare a Cloud Computing Risk Assessment to identify potential cyber security risks that are introduced to the environment. The FAA will also revise the existing Cyber Security Architecture to adequately protect the FAA from potential risks and threats from the adoption of cloud services. Additional risks and challenges from cloud computing include the capacity and readiness of existing network infrastructure, interoperability, integration with existing systems, and technology maturity. Cloud services are delivered over a network and the FAA will conduct engineering studies and analysis to make cloud deployment model decisions and ensure that response-time and bandwidth requirements will not impact negatively the performance and normal operations of FAA IT systems. The adoption and migration to cloud services in the FAA will be an incremental process and it requires co-existence, interoperability and integration with existing systems to avoid disruption of FAA operations. The FAA will also evaluate and identify the need for technology pilots and proof-of-concept programs to manage and minimize risks and challenges from the adoption of cloud services. Objectives to manage technical risks include:

- Develop an enterprise cloud computing risk assessment to identify potential risks introduced to the FAA IT environment,
- Implement a cyber security architecture to adequately protect the FAA IT environment from growing and evolving cyber security threats ,
- Analyze the current network capacity and make cloud model choices and implementation architecture decisions to ensure that cloud computing will not represent a bottleneck to network services, and
- Conduct technology pilots and proofs-of-concept to manage and minimize risks to the FAA IT environment.

A critical success factor for the adoption of new approaches and technologies including cloud computing services is to adequately address the management aspects of the transition including communication, outreach and training. The FAA will ensure that stakeholders are well informed and their concerns and expectations are properly addressed. The FAA will develop and execute a communications strategy and plan, conduct outreach activities, train stakeholders, and clearly define roles and responsibilities. The shift in the way to create, provide and consume IT services may create the need to train IT users and stakeholders. Objectives include:

- Develop and implement a cloud computing communication, outreach and training plan. The FAA will identify stakeholders and their communication, outreach and training needs. It will develop appropriate material to satisfy those needs.

In addition, Federal IT programs and initiatives need to comply with overall Federal mandates, rules and regulations. There are also specific policies, rules and regulations to support the adoption of cloud computing in the federal government. The FAA will develop internal policies, rules and regulations that are required to ensure a secure and reliable FAA IT environment. The FAA will establish the appropriate mechanisms to monitor and control compliance of all these external and internal mandates, rules and regulations (OMB, NIST, FedRAMP, FAA, DOT, etc.).

# 5. FAA Cloud Computing Initiatives

The FAA is currently working on cloud computing initiatives at different levels of detail across its two major domains: NAS and non-NAS. Given the different objectives and characteristics of the two domains, it is expected that different implementation strategies and initiatives will be required for each domain while maintaining alignment with the unified FAA's cloud computing direction and strategy. It is also expected that NAS and non-NAS domains will continue to collaborate and take advantage of potential economies of scale and synergies among their implementation strategies and initiatives.

The FAA's non-NAS Air Traffic Organization (ATO) IT is one of the offices leading deployment of cloud technology in the Agency. The following are key current initiatives that are managed by the non-NAS domain; in addition to providing services to meet non-NAS requirements, these initiatives may offer services for NAS requirements in the future:

- The FAA plans to move its current Lotus Notes email system to the cloud, and it is in the process of evaluating and selecting an enterprise email cloud provider via a public Screening Information Request/Request for Offer (SIR/RFO). Once awarded, FAA will migrate from its current email system to the new system following the terms of the new contract. Once completed, FAA will join the ranks of other federal agencies which have moved to cloud-based email services.
- FAA is working to pursue cloud computing opportunities via data center initiatives. Over-arching, long term strategy here is the FAA Data Center Consolidation Initiative (DCCI). This is a large, multi-year investment program that assesses and will select alternatives for our data center future. This builds on known past cost savings from server consolidation, server virtualization, and some data center consolidation. The FAA DCCI is a core component of FAA's NextGen Facilities transformation initiative, and part of the DCCI is to provide data center cloud services in the future. In addition to the long term DCCI program, FAA has a short-term pilot program initiative involving data center IaaS capabilities in Herndon, VA. FAA is in the unique position to repurpose its Herndon, VA facility into a consolidated data center and begin hosting a community cloud as a shared resource for government agencies. A key step in migrating to the cloud is to take those FAA applications which are the lowest risk, and are already virtualized, and transfer them from existing FAA data centers to the Herndon Data Center. In addition to server virtualization and consolidation, the Herndon facility will offer a self-service interface in which customers can request their own infrastructure and provision it based on the need of the project. The results of this pilot initiative will provide lessons learned to the DCCI program as it assesses longer term data center and cloud computing alternatives for FAA.
- The FAA has also contracted with cloud service provider Akamai to provide seamless, on demand FAA.gov web content delivery to the flying public, aviation industry, and other government agencies. Key objectives for this contract are to provide on-demand instant scalability for handling surge-type events (e.g. "Miracle on the Hudson" transcripts and audio), provide protection to FAA's web infrastructure against Distributed Denial of Service (DDOS) attacks, optimize delivery of web content through application acceleration, and reduce total cost

of ownership by offloading network services. The Agency estimates costs savings of $2.2 million per year.

On the NAS domain, the FAA's NAS ATO has started strategy and planning activities and is in the process of defining its cloud computing strategy and plan. The NAS is also developing a Cloud Computing Suitability Assessment Tool to determine the suitability of programs for using cloud services. The FAA has used cloud pilot projects and prototypes to gain an understanding of the cloud computing environment and will leverage this knowledge for future implementations. Cloud computing is in the early phases of development and within that context, the FAA has made significant progress to date; at the same time, the Agency recognizes that there is abundant work left to explore and capture cloud computing benefits across the Agency. This strategy document provides the high-level direction to continue deploying cloud computing technology in the Agency. Initial suitability assessments are being conducted across the initial list of OMB's selected programs using the Cloud Suitability Tool. In accordance with the FAA Cloud Computing Strategy, additional detailed analysis is planned and required. Figure 4 is presented as a sample of a next level analysis and planning activities that may need to be performed by the FAA to execute this strategy.

Figure 4 is notional and it provides a visualization of sample activities for the introduction of cloud computing technology to the FAA. It also identifies the potential value and level of risk to the organization. This or a similar tool can be employed by the FAA to perform detailed planning activities to support and enable the FAA Cloud Computing Strategy.

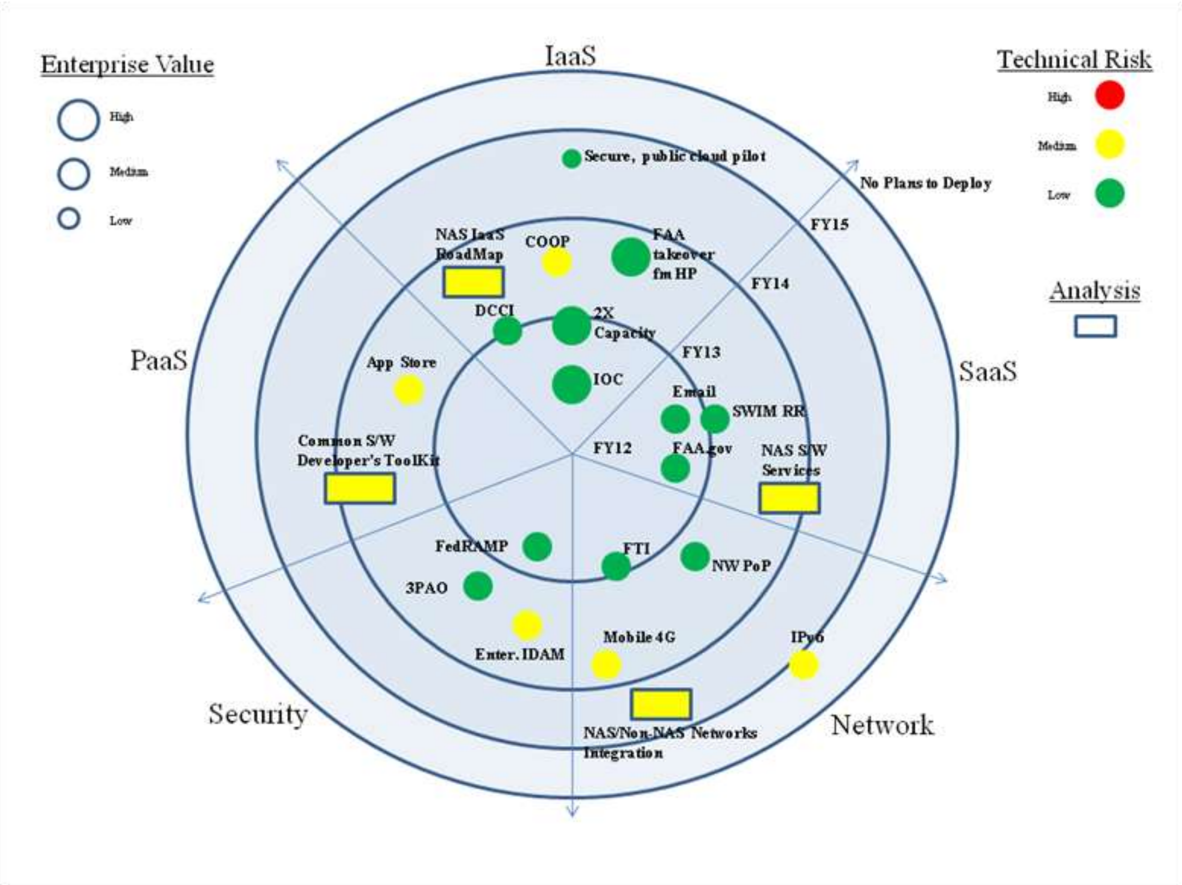


**Figure 4. Cloud Computing Technology Introduction (Notional with Sample Activities)**

The figure shows notional and sample activities for the three cloud service types (IaaS, PaaS, SaaS). It also includes Security and Network sample activities that may be required to enable and support IaaS, PaaS, and SaaS. The concentric circles represent time: for example, the smaller circle may represent FY 2012, and all the activities identified within that circle need to be completed by the end of FY 2012. The rectangles represent analysis activities that are required in each of the dimensions of the figure. Value to the FAA is represented by the activity circle size. Risk level to the FAA is represented by color: Green (Low), Yellow (Medium), and Red (High).

# 6. FAA Cloud Computing Strategy Implementation

The approach to guide and achieve the FAA Cloud Computing strategic goals includes the following characteristics:

- FAA-wide scope, owned, driven and supported by senior FAA executives. Cloud computing has an FAA-wide, multi-functional, multi-organizational impact. It requires the sponsorship, leadership and direction from senior leaders to succeed. It requires an FAA-wide perspective to take advantage of economies of scale, avoid the creation of IT silos, and capture cloud computing benefits in support of the FAA's mission and goals.
- Implementation that has measurable value. The FAA migration to cloud services will be practical and it will demonstrate value and benefits to the FAA including cost efficiency, increased IT provisioning speed, and IT complexity reduction. The FAA will also identify opportunities to provide and demonstrate tangible and robust value early in the cloud adoption and migration process.
- Incremental implementation, to manage risk. The FAA will use an incremental approach to moving systems and programs to a cloud computing environment to ensure all IT systems remain secure and reliable, and that the adoption of cloud services does not introduce unnecessary risks to the FAA IT environment. The FAA will establish a balanced approach to evaluate risk and potential value when making cloud service migration and adoption decisions. Low risk, high value services are likely candidates to migrate early in the process. Higher risk services will be the subject of additional analysis, and they will be considered for later phases in the process.
- Collaboration across FAA organizations and programs. The adoption of cloud services has the potential to impact all elements of the FAA organization. A collaborative, cross-functional, cross-organizational approach will be used. The adoption and migration of cloud services will require the work and collaboration of multiple FAA organizations including those with responsibility in systems engineering, the AMS life cycle, Enterprise Architecture, cyber security, software development, and program management.

The FAA is currently using SOA to modernize some of its systems. The common, natural, and effective way to facilitate access to cloud services is using SOA principles and technologies. The FAA will take advantage and leverage current investments in SOA infrastructure to adopt cloud computing. SOA will be an essential part of cloud computing adoption across the FAA.

Organizations within the Federal Government, including OMB, National Institute of Standards and Technology (NIST), General Services Administration (GSA), and Department of Homeland Security (DHS), have developed and continue to develop cloud computing resources and guidance including issues related to security, procurement, and standards. The FAA will leverage these resources to expedite the process of evaluating, selecting, acquiring cloud computing capabilities, and mitigating risks.

In accordance with the risk-based incremental approach, the FAA Cloud Computing Strategy has initially identified three phases for the adoption and migration of cloud services. These phases include specific FAA activities and outcomes over time, while maintaining compatibility and alignment with the overall Federal Cloud Computing Strategy. It is important to highlight that the FAA's cloud computing approach represents a solid commitment to capture cloud computing benefits for the Agency while maintaining the secure, safe and reliable environment that the FAA requires to fulfill its mission. Phases are primarily aligned with risk, and significant transformation to cloud services may occur during the early phases if it is determined that they provide high value and they do not represent an unacceptable level of risk to the FAA IT environment. The scope and number of phases may be adjusted in the future to reflect federal and FAA's priorities and funding levels. The FAA Cloud Computing Strategy includes the following phases:

**Phase 1: Foundation (establish the initial capability)**

The goal of this phase is to establish a solid foundation to position the FAA to successfully capture the benefits of cloud computing across the Agency. This phase will also include the identification and migration of low-risk, high-value cloud services that can deliver and demonstrate early value to the FAA. The FAA will work on organizational, process and technology elements to support the definition and establishment of a solid cloud computing foundation. Key outcomes during this phase include:

- Initial assessment and selection of cloud services,
- Concept of Operations document,
- Roadmap and plan for migration including the planned retirement of legacy IT replaced by cloud services,
- Initial policies, processes and governance including enterprise credit in investments for first adopters to enable cloud migration roadmap, and
- Migration of selected low-risk and high-value cloud services.

A key characteristic of the implementation approach is to provide early and tangible value to the Agency (quick wins). During this initial phase, the FAA will identify and migrate to the cloud selected services that provide high-value and represent low-risk to the FAA. To achieve this, the FAA plans to perform the following activities early during Phase 1:

- Identify high-value and low-risk opportunities to take advantage of IaaS. Infrastructure components including storage, virtual machines (UNIX, LINUX, Windows, etc.), and Web hosting are typically commoditized items and some infrastructure pieces may be selected and migrated to cloud services with low levels of risks and high potential value to the FAA.
- Identify high-value and low-risk opportunities to take advantage of PaaS. High development costs and complexity are two critical items for CIOs across IT organizations and the FAA. Some

software development organizations across the FAA may take advantage of cloud development platforms and toolkits to allow cost reduction with an adequate level of risk to the organization.

- Identify high-value and low-risk opportunities to take advantage of SaaS. Standardized business processes including some administrative and business systems are good candidates for cloud adoption. Some systems may already be provisioned by external parties, and they may have relatively simple requirements for security, privacy and performance.
- Select and migrate cloud services. The FAA will select the most appropriate deployment model (private, public, community, or hybrid) to balance value and risk to the Agency. As part of the migration process, the FAA will also modify policy and governance processes as required to enable the cloud services. For instance, a new policy may be required to direct organizations to use selected cloud services, and governance processes will be required to support the policy.

As part of phase 1, FAA has begun transition of the FAA's e-mail system to the cloud. The FAA's (non-NAS) private and/or federal community cloud services at Herndon will also be a key part of phase 1. Part of the detailed assessment and selection during this phase will include the consideration and analysis of the ability and capability of the non-NAS private cloud to satisfy NAS requirements including security, privacy, reliability and performance.

Due to the stringent security, safety, reliability and performance requirements of the NAS, a solid and robust systems engineering approach will be required to minimize risks and avoid disruption of the NAS operations. The NAS components that are found suitable for cloud services during the detailed analysis will be targeted to begin migration activities during the last phase of this strategy implementation.

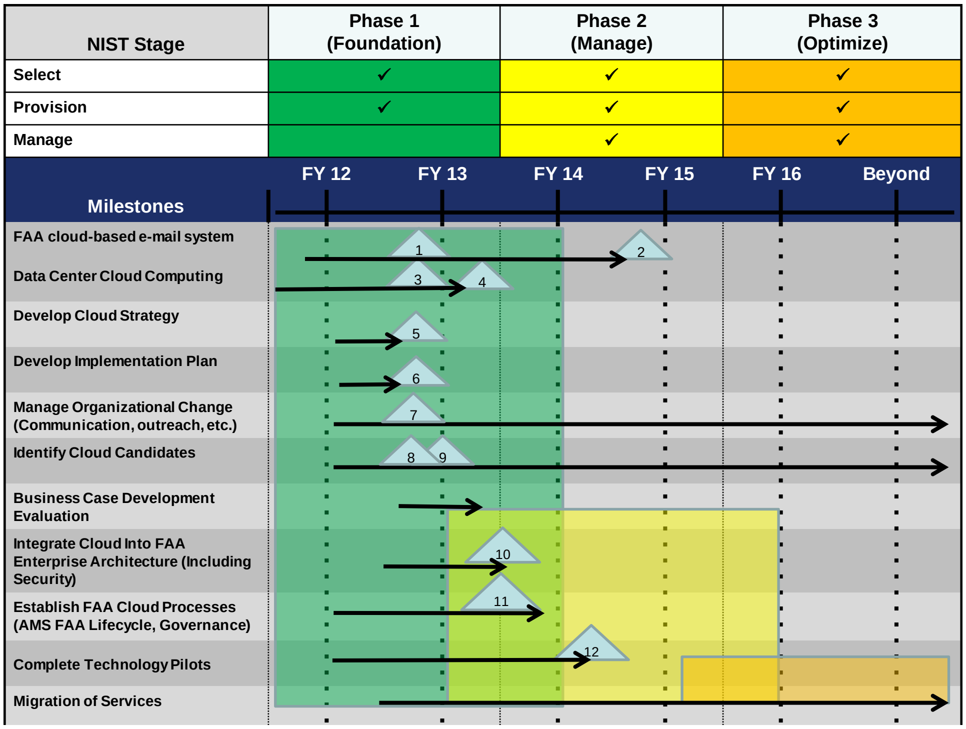
**Phase 2: Manage (mature practices and technologies)**

The goal of this phase is to develop more mature practices and technologies that support adoption and migration of cloud services that represent a higher level of risk to the organization. The Phase 1 analysis will determine cloud services that are candidates for migration during this phase, but potential candidates may include some FAA non-NAS and NAS regulatory systems with relatively low demands for security, privacy and performance. Key outcomes during this phase will include a robust cloud and security architecture, revised processes, and governance to enable the cloud migration roadmap, and migration of selected cloud services.

**Phase 3: Optimize (move higher risk operations to cloud)**

The goal of this phase is to increase maturity levels of practices, technologies and organization that allow the FAA to confidently migrate cloud services that represent the highest risk to the fulfillment of the FAA's mission and goals. The Phase 1 and 2 analyses will determine the cloud services that are candidates for migration during this phase, but potential candidates may include selected FAA NAS systems with strict security, privacy and performance requirements. Key outcomes during this phase will include a revised robust cloud and security architecture to support selected air traffic management and control systems, revised processes and governance to enable the cloud migration road map, and the migration of selected services.

Figure 5 summarizes the high level roadmap for the FAA Cloud Computing Strategy. The current roadmap is notional and its timeline will depend on Federal and Agency priorities, and funding availability.



| NIST Stage | Phase 1 (Foundation) | Phase 2 (Manage) | Phase 3 (Optimize) |
|---|---|---|---|
| Select | ✓ | ✓ | ✓ |
| Provision | ✓ | ✓ | ✓ |
| Manage | | ✓ | ✓ |

| ID | Milestone |
|---|---|
| 1 | E-mail system contract award – Contract is awarded to selected E-mail cloud service provider |
| 2 | E-mail system migration completed – Lotus Notes users are migrated to new E-mail system |
| 3 | Herndon IaaS Pilot Initial Operating Capability (IOC) |
| 4 | Final Investment Decision (FID) for the Data Center Consolidation Initiative (DCCI) |
| 5 | Complete and approve FAA Cloud Computing Strategy – Approved by CIO and Senior Executives |
| 6 | Complete and approve Concept of Operations and Implementation Plan |
| 7 | Complete organization change management plan – Communications, outreach and training |
| 8 | Complete initial assessment (quick wins) – Opportunities with high value and low risk |
| 9 | Complete detailed assessment – Comprehensive assessment, vertical and horizontal analysis |
| 10 | Define target architecture and cloud migration roadmap (including security) |
| 11 | Complete program guidelines for cloud migration |
| 12 | Conduct technology pilots, including the Herndon IaaS Pilot – Risk reduction |

**Figure 5. FAA Cloud Computing Strategy Roadmap**

# *7. Cloud Computing Challenges*

While cloud computing offers many potential benefits to the FAA, several challenges exist in its application. The FAA will balance risks and benefits when evaluating and using cloud computing. Security and performance are two key existing technical challenges in the application of cloud computing. NAS and non-NAS systems have different requirements for security and performance, and it is expected that they will need different tactical plans to address and mitigate these risks. The main cloud computing challenges are described in the next paragraphs.

## Security Challenges

The FAA has a continuing requirement for secure and trusted cloud computing capabilities. The FAA cloud computing security requirements will meet the Federal Information Security Management Act (FISMA) requirements that include but are not limited to: compliance with Federal Information Processing Standards agency specific policies; Authorization to Operate (ATO) requirements; and vulnerability and security event monitoring, logging, and reporting.

The FAA will consider security needs across a number of dimensions, including but not limited to:

- Statutory compliance to laws, regulations, and agency requirements
- Data characteristics to assess which fundamental protections an application’s data set requires
- Privacy and confidentiality to protect against accidental and nefarious access to information
- Integrity to ensure data is authorized, complete, and accurate
- Data controls and access policies to determine where data can be stored and who can access physical locations
- Governance to ensure that cloud computing service providers are sufficiently transparent, have adequate security and management controls
- Physical facility security.

A key to secure use of cloud computing is the shared understanding of the division of security responsibilities between provider and client, and the ability to verify that both are meeting their responsibilities. Methods for doing this include contract clauses that are specific to cloud computing as well as service level agreements that spell out security and privacy requirements.

The FedRAMP CONOPS makes clear that a third party assessor (3PAO) role is important to assess the security controls implementation of a cloud service provider (CSP). This is written in the context of formal accreditation of a commercially run cloud service. FAA is initially running a different model, a *private* cloud, operated with internal IT personnel. The spirit of the FedRAMP CONOPs Third Party Assessor role is an independent verification and validation of a cloud service, from a security firm that has been qualified by GSA to perform this work. The FAA will comply with the spirit of the CONOPS when the FedRAMP program qualifies providers of the 3PAO service, and contract for an independent security assessment from a 3PAO. FAA will accordingly update its security procedures and tools based on results of the assessment.

FAA has robust, FISMA compliant procedures for identity management and access control and is in the process of federating those network identity credentials across its enterprise as a necessary security control for a cloud-centric architecture. Additional information regarding the challenges of cloud computing security is provided in Appendix B.

## Performance Challenges

One characteristic of cloud computing is to deliver services over a network, typically a Wide Area Network (WAN), such as the Internet. While this characteristic provides benefits, it also presents a critical challenge, especially for systems like the NAS with real-time and strict performance requirements. At the present, there is a lack of understanding and information on how NAS systems can perform in a public cloud computing environment. Cloud computing performance analysis on candidate architectures and benchmark data should support the cloud suitability, and investment analysis and decision process.

## Other Challenges

In addition to security and performance, there are other challenges that the FAA needs to consider for the successful deployment of cloud technology. The following challenges are not technical "show stoppers"; rather, they are procedural, accounting-related or cultural challenges that can be overcome with effort.

Some of the challenges for attaining success with cloud computing include:

- Historically, the leasing of IT equipment has not proved cost-beneficial. In some ways, cloud computing can approximate leasing. If one has servers at high utilization rates, in conjunction with server virtualization that yields multiple server instances for each physical server machine, then it is difficult for a cloud IaaS vendor to compete with in-house server costs when both are on a 24x7 schedule. However, cloud IaaS vendors can be competitive when servers and/or storage are at low utilization levels. We plan to mitigate this through our cloud suitability assessment framework.

- If cloud computing benefits rest on freeing up data center physical space and/or electricity consumption, then those savings usually accrue outside of FAA, such as to GSA. For FAA to see those benefits, we become dependent on GSA reducing its charges for the associated office space and power. Usually, GSA is not willing to do this, at least not in the short term. This hinders capturing benefits.

- If a PaaS capability is acquired, then typically this adds another infrastructure platform to one's portfolio of existing investments in system software and hardware (platforms). The PaaS capability may not be the same as internal system software or platform. This can add yet another system maintenance environment to manage over time and can lead to greater complexity in one's portfolio of IT infrastructure. This can make interoperability more difficult. To mitigate this, we can consider constraining the number of added platforms that are acquired through cloud computing and/or focus on platforms that are similar to or compatible with existing FAA platforms.

- Portability – There is a risk of vendor lock-in once an organization has moved a workload to a public cloud vendor. It is important to avoid lengthy vendor lock-in, as an increase in the ability to move from one vendor to another implies that the infrastructure is behaving more like a utility for services. Moving that workload at a future point in time can be problematic since the platform is somewhat unique and may not be easily replicated. Also, there is a lack of standards for cloud computing, though these may emerge in the future. NIST is actively working on standards for cloud computing. The federal government will benefit from adopting and implementing standards for cloud portability and interoperability.
- Cloud computing can lead to a sense of infinite computing resource availability which, in turn, can eventually foster escalating costs over time. This involves the risk of cost increases either from increased usage and/or increased fees.
- Cloud computing implies a shift in funding from capital expenditures toward operational expenditures. At FAA, this involves a shift from F&E funding to Ops funding. Shifting budgets in this manner can prove difficult. Also, initial adoption of cloud computing may require upfront capital expenditures

Today, there are some concerns in the use of a *public* cloud computing model, especially when IT systems and infrastructure holding sensitive data and with strict requirements for safety, security, privacy, reliability and performance are involved. The FAA will continue to work with industry and relevant government agencies leading federal security requirements for cloud computing to address these concerns and ensure that the FAA IT environment is safe, secure and reliable. For instance, the FAA is aware through contact with NIST and the National Security Agency (NSA) that there are technical projects underway to enable public cloud vendors to host a "government" cloud, a *public* IaaS service. The FAA may use for strategic planning purposes the assumption of near-term availability of an expected USG *public,* accredited secure cloud. The FAA will add to its strategy in future updates a pilot project with an approved *public* government cloud offering, and in the future will consider moving non-safety-critical, non-operationally-critical information and services to a *public* cloud model. *Public* cloud vendors argue that their service offerings must be lower cost to an organization than a *private* cloud simply because of the efficiency of spreading the infrastructure cost across a large customer base. While this argument is appealing, there has not been much data available to verify this. The FAA expects to be in a position to judge the best economic tradeoff, in addition to security and data latency, after operating its *private* cloud for a year.

# *APPENDIX A: Cloud Computing Overview*

The FAA is using the NIST definition of cloud computing. The National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, provides the following definition of cloud computing in NIST Special Publication 800-145 (NIST SP 800-145):

> "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The NIST cloud model promotes availability and is composed of **five essential characteristics, three service models, and four deployment models**".

Cloud computing provides the rapid delivery of computing resources inexpensively to multiple users from a centralized source of related and unique service offerings that is shared by many customers. This is summarized in Figure A-1.

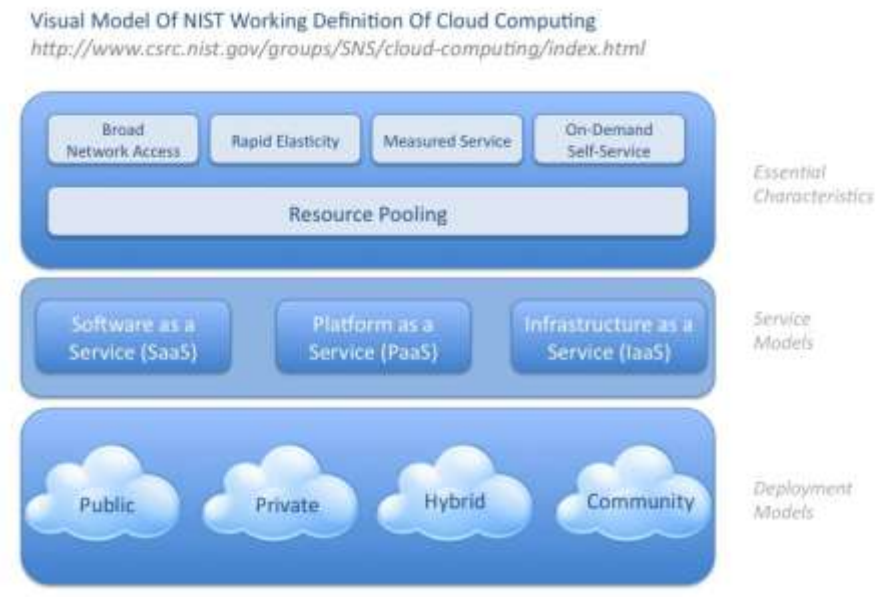

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html
Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Resource Pooling
Essential Characteristics
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Service Models
Public
Private
Hybrid
Community
Deployment Models

**Figure A-1: Visual Model of NIST Definition of Cloud Computing (from CloudSecurity Alliance.org)**

NIST describes the following *five primary essential characteristics* of cloud computing:

1. **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider. This involves online provisioning.

2. **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms. For *public* clouds, this includes use of the Internet. For *private* clouds, this typically involves enterprise Wide Area Networks (WANs) supplemented with local area networks (LANs).

3. **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

4. **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time. This is generally true of *public* cloud offerings and lesser flexibility is offered in other cloud models because total flexibility comes at a price that a large *public* cloud vendor can amortize over a million cloud customers (e.g., Amazon Web Services), which cloud models with only dozens of internal customers cannot match.

5. **Measured Service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

NIST also identifies *three discrete service offerings*, each of unique value to the customer. As customers move up this offering chain, they gain greater efficiencies, yet more standardization is required:

1. **Cloud Infrastructure as a Service (IaaS).** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer neither manages nor controls the underlying cloud infrastructure but has control over choice of operating system, storage size, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). This model provides the most flexibility for the customer, however will not provide all the potential efficiencies gained at the Software as a Service (SaaS) model.

2. **Cloud Platform as a Service (PaaS).** The capability allows customers to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. These applications pull computing resources as needed by the underlying platform and are metered for the computing resources they actually use. The consumer neither manage nor controls the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. PaaS is an excellent application development environment where real-time collaboration among teams of disbursed developers is the norm.

3. **Cloud Software as a Service (SaaS).** The capability provided to the consumer is to use the *provider's* applications running on a cloud infrastructure. The consumer neither manages nor controls the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Among the three services, statistics at the end of 2011 show that SaaS is the dominant cloud service in use in the commercial world garnering about 87% of the cloud market (source, Network World).

Finally, NIST identifies *four primary deployment models*, which are generally accepted across government. These deployment models range from models that are more secure to those that are more available. Federal agencies will employ models based on risk-based decisions that address their financial, operational, and security needs. The four models include:

1. ***Private* cloud.** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
2. ***Community* cloud.** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
3. ***Public* cloud.** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
4. ***Hybrid* cloud.** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

The primary differences among these models are in scope and access.

# *APPENDIX B: Cloud Computing Security Challenges*

In computer security incidents there are typically three types of actors: the Malicious Insider, the Malicious Outsider, and the well-meaning Insider.  A data security breach usually involves a combination of more than one of these types of actors. For example, a malicious outsider sends an email to a well-meaning insider and that insider inadvertently opens an attachment and unleashes MALWARE. Alternately, a malicious insider provides insider access control and identity management data to a malicious outsider, who uses it to access a network and data that he/she is unauthorized for use. The key feature to notice in these scenarios is that one of the actors resides on the Internet, and at least one of the other actors resides on an IP network, where the sensitive information is hosted, that can access data to/from the Internet.

FAA has taken strong measures to prevent data breaches through operation of a closed wide-area network, Federal Telecommunications Infrastructure (FTI). The NAS programs are on FTI. The FAA *private* cloud at the Herndon data center will be on FTI, and will not be Internet-facing. Although the reality of long-haul Internet Protocol packet transmission is that unless an organization owns the physical fiber optic cables in the ground, at the physical layer there is packet mingling with Internet traffic. In the case of FTI, the network is logically separated from the rest of the Internet because the end user Internet Protocol (IP) addresses are privately routed addresses. This means that the routers that form the traffic managers on the FTI network will not pass a packet from outside of FTI, that is, from the Internet, onto FTI.

Embracing any other form of cloud computing service model other than the *private* cloud would expose the FTI network directly to the Internet. This is an unacceptable risk to real-time operations of the NAS and to ensuring passenger safety.

## FAA Cloud Service Model Security Compliance

The FAA has a continuing requirement for secure and trusted cloud computing capabilities.  The FAA cloud computing security requirements will meet the Federal Information Security Management Act (FISMA) requirements that include but are not limited to: compliance with Federal Information Processing Standards agency specific policies; Authorization to Operate (ATO) requirements; and vulnerability and security event monitoring, logging, and reporting.

The FAA will consider security needs across a number of dimensions, including but not limited to:

- Statutory compliance to laws, regulations, and agency requirements
- Data characteristics to assess which fundamental protections an application’s data set requires
- Privacy and confidentiality to protect against accidental and nefarious access to information
- Integrity to ensure data is authorized, complete, and accurate
- Data controls and access policies to determine where data can be stored and who can access physical locations
- Governance to ensure that cloud computing service providers are sufficiently transparent, have adequate security and management controls”

- Physical facility security

A key to secure use of cloud computing is the shared understanding of the division of security responsibilities between provider and client, and the ability to verify that both are meeting their responsibilities. Methods for doing this include contract clauses that are specific to cloud computing as well as service level agreements that spell out security and privacy requirements.

FAA has robust, FISMA compliant procedures for identity management and access control and is in the process of federating those network identity credentials across its enterprise as a necessary security control for a cloud-centric architecture.

While establishing a cloud security architecture, the FAA considered the following sources of cloud information:

- NIST Special Publication **800-53, Revision 3**, *Recommended Security Controls for Federal Information Systems and Organizations*
- Special Publication **800-125**, *Guide to Security for Full Virtualization Technologies*, January 2011
- Draft Special Publication **800-144**, *Guidelines on Security and Privacy Issues in Public Cloud Computing*, January 2011
- Draft Special Publication **800-145**, *NIST Definition of Cloud Computing*, January 2011
- Draft Special Publication **800-146,** *Cloud Computing Synopsis and Recommendations,* May 2011
- NIST USG Cloud Computing Technology Roadmap Vol.III, *Technical Considerations for USG Cloud Computing Deployment Decisions, November 2011*
- FedRAMP CONOPS, V.1.0, *February, 2012*

## FedRAMP Concept

The FedRAMP CONOPS makes clear that a third party assessor (3PAO) role is important to assess the security controls implementation of a cloud service provider (CSP). This is written in the context of formal accreditation of a commercially run cloud service. FAA is running a different model, a *private* cloud, operated with internal IT personnel. The spirit of the FedRAMP CONOPs Third Party Assessor role is an independent verification and validation of a cloud service, from a security firm that has been qualified by GSA to perform this work. FAA will comply with the spirit of the CONOPS when the FedRAMP program qualifies providers of the 3PAO service, and contract for a security assessment. FAA will accordingly update its security procedures and tools based on results of the assessment.

# APPENDIX C: Acronyms

Selected acronyms and abbreviations used in the document are defined below.

| | |
|---|---|
| **3PAO** | Third Party Assessor |
| **ACAT** | Acquisition Category |
| **AMS** | Acquisition Management System |
| **ATCSCC** | Air Traffic Control System Command Center |
| **ATO** | Authorization to Operate |
| **CIO** | Chief Information Officer |
| **CIP** | Critical Infrastructure Protection |
| **CRD** | Concept and Requirements Definition |
| **CSP** | Cloud Service Provider |
| **CUI** | Controlled Unclassified Information |
| **DCCI** | Data Center Consolidation Initiative |
| **DDOS** | Distributed Denial of Service |
| **DHS** | Department of Homeland Security |
| **DOT** | Department of Transportation |
| **EA** | Enterprise Architecture |
| **F&E** | Facilities and Equipment |
| **FAA** | Federal Aviation Administration |
| **FedRAMP** | Federal Risk and Authorization Management Program |
| **FIPS** | Federal Information Processing Standards |
| **FISMA** | Federal Information Security Management Act |
| **FTI** | Federal Telecommunications Infrastructure |
| **GSA** | General Services Administration |
| **IaaS** | Infrastructure as a Service |
| **IARD** | Investment Analysis Readiness Decision |
| **IID** | Initial Investment Decision |

| | |
|---|---|
| **IOC** | Initial Operating Capability |
| **IP** | Internet Protocol |
| **IT** | Information Technology |
| **MMAC** | Mike Monroney Aeronautical Center |
| **NAS** | National Airspace System |
| **NextGen** | Next Generation Air Transportation System |
| **NIST** | National Institute of Standards and Technology |
| **NSA** | National Security Agency |
| **OCIO** | Office of the Chief Information Officer |
| **OMB** | Office of Management and Budget |
| **Ops** | Operations |
| **PaaS** | Platform as a Service |
| **PHI** | Protected Health Information |
| **PII** | Personally identifiable information |
| **PM** | Program Manager |
| **RFO** | Request for Offer |
| **SaaS** | Software as a Service |
| **SIR** | Screening Information Request |
| **USG** | United States Government |
| **WJHTC** | William J. Hughes Technical Center |