US FEDERAL AGENCIES AND CLOUD: A COMMON DECISION FRAMEWORK FOR DETERMINING WHICH LEGACY IT SYSTEMS SHOULD MIGRATE TO CLOUD

by

Allan L. Mink II

A Dissertation
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
The Requirements for the Degree
of
Doctor of Philosophy
Information Technology

Committee:

_____	Dr. Peggy Brouse Dissertation Director
_____	Dr. Stephen Nash Committee Member
_____	Dr. David Schum Committee Member
_____	Prof. Paul Strassmann Committee Member
_____	Dr. Stephen Nash Senior Associate Dean
_____	Dr. Kenneth S. Ball Dean, Volgenau School of Engineering

Date: _____ Spring Semester 2015
George Mason University
Fairfax, VA

US Federal Agencies and Cloud: A Common Decision Framework for Determining Which Legacy IT Systems Should Migrate to Cloud

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at George Mason University

by

Allan L. Mink II
Master of Science
Carnegie-Mellon University, 1980
Bachelor of Science
Massachusetts Institute of Technology, 1978

Director: Peggy Brouse, Associate Professor
Volgenau School of Engineering

Spring Semester 2015
George Mason University
Fairfax, VA

DEDICATION

This is dedicated to my loving wife Sue, my two wonderful children Jess & Rob.

ACKNOWLEDGEMENTS

I would like to thank the many friends, relatives, and supporters who have made this happen.

My loving wife Sue, who supported me throughout this marathon and personally slaved for uncounted hours transcribing many interviews and serving as technical editor for the written dissertation. My parents, Jan and Al Mink Sr. who sparked my passion to discover and learn about the nature of things.

My advisory committee -- Drs. Brouse, Schum, and Nash, along with Prof Strassmann of my committee were of invaluable help with their research expertise as well as their support as I worked through the PhD process.

A special acknowledgement as a memorial for Dr. Sage, who inspired me to apply a systems engineering approach to my research and who served as my research director till the time of my dissertation writing.

Others who contributed time and support -- Dr. Rose Noxon who provided coaching, tips and motivation throughout this journey. Susan Mueller and Lisa Nolder, who helped me navigate the maze of the GMU academic process.

The senior leaders in our Federal Government who facilitated access to the three key case studies: Mr. Roger Baker, former Chief Information Officer (CIO) of Veterans Affairs, Lt Gen Jeff Sorrenson, former Army CIO, and Mr. Errol Arkilic, Program Director at the National Science Foundation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

US FEDERAL AGENCIES AND CLOUD: A COMMON DECISION FRAMEWORK FOR DETERMINING WHICH LEGACY IT SYSTEMS SHOULD MIGRATE TO CLOUD

Allan L. Mink II, PhD

George Mason University, 2015

Dissertation Director: Dr. Peggy Brouse

Cloud is a disruptive wave in information technology (IT), much like the mainframe, PC, and internet waves preceding it. As with the past disruptive waves, Cloud promises great potential and significant risks for IT leaders in the US Federal Government. Federal Agencies spend $80B annually developing, modifying, and sustaining over 12,000 IT systems using traditional (non-Cloud) information technology (IT) methods. Cloud offers US Federal Agencies the potential to reduce costs while improving their capabilities.

Understanding the need for US Federal Agencies to make better use of Cloud, the former US Federal CIO (Vivek Kundra) directed Federal Agencies to pursue a "Cloud First" policy and proposed a Cloud decision framework referred to in this paper as the US Federal Cloud Decision Framework (USFCDF). Vivek departed for a position at Harvard University before his USFCDF was adopted.

Federal Agencies have been reluctant to adopt Cloud. A recent analysis by the US Government Accountability Office (GAO) determined that in 2014, that only 2% of the IT budget of the agencies it studied was spent on Cloud. The remainder paid for traditional legacy IT systems and their management. Furthermore, Congress held up one Cloud migration because they felt the Agency lacked rationale for their Cloud migration decision. Another Agency cancelled their Cloud migration just as it started because their Inspector General felt that the Cloud migration decision did not adequately consider some important factors. The slow adoption and challenges to some of those few Cloud migration decisions indicate the US Government is stumbling with this new disruptive wave of technology. The problem is that *US Federal Agencies lack a common, validated decision framework for deciding whether a legacy IT system should migrate to the Cloud.* This paper supports the hypothesis that *the USFCDF proposed by Kundra provides value to Federal IT decision makers in determining whether a well-defined legacy IT system should migrate to the Cloud.*

To validate such a conclusion, this research project applied multiple-case study methodology to examine the decisions made by five Federal Agencies to migrate a legacy IT system (email) to the Cloud. The research project compared how these actual decisions related to the USFCDF.

The research project leveraged related theory, such as the the definitions and models related to Cloud as documented by the US National Institute of Standards and Technology (NIST). The research project also marshalled the findings from the case studies into a Wigmore inference model (Kadane 1996), linking the case study evidence

to the hypothesis through the use of Araucaria, a software tool for argument analysis, diagramming, and representation developed by the Division of Applied Computing, University of Dundee.

The results of the research indicate that in each of the five migration decisions studied the Federal Agency independently developed their own decision frameworks without the benefit of being informed by the USFCDF. However, by comparing each decision against the USFCDF, this research project discovered similar alignments, suggesting that USFCDF could serve as a common framework for Cloud migration decisions. Insights from this research indicate how Kundra's original proposal could be evolved and adopted Government. The validation and refinement of the USFCDF should help decision makers make better decisions about Cloud. And, by adopting a uniform decision framework, the US Federal Government should benefit collectively through the body of knowledge accumulated from past decisions captured in a consistent, widely adopted framework.

1. INTRODUCTION

Cloud is becoming recognized as a disruptive wave in information technology (IT), much like the mainframe, PC, and internet waves preceding it. In their collection of works about how information and IT have affected the United States, Alfred Chandler and James Cortada depict the three waves proceeding Cloud in Figure 1.

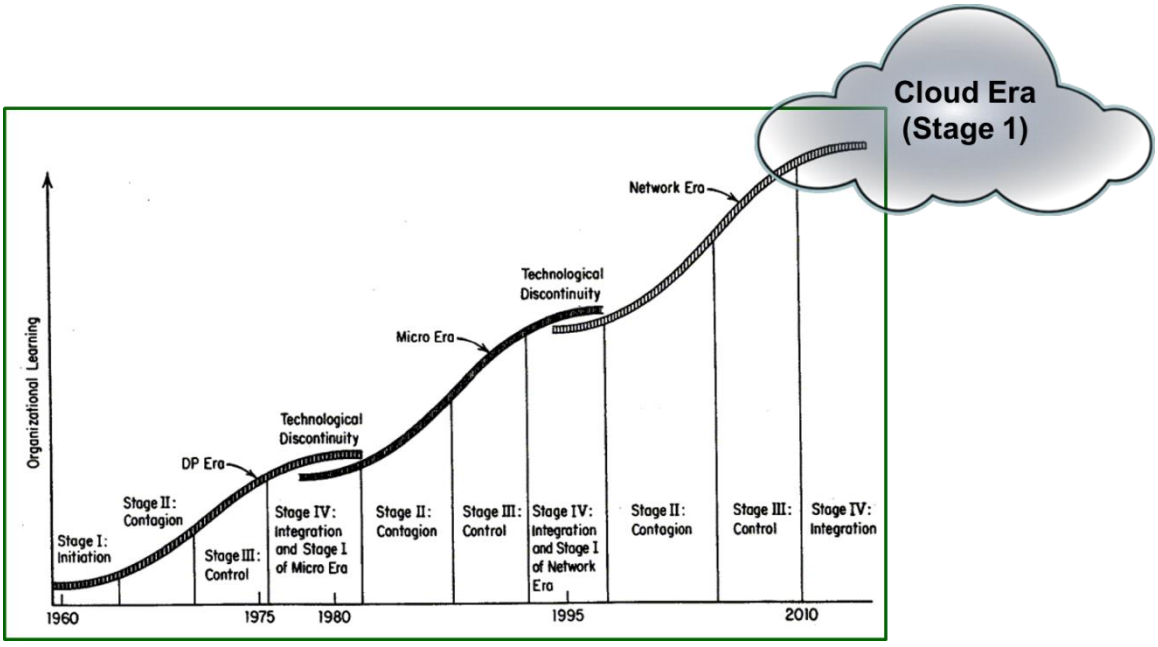


Figure 1 - Technology Waves and Cloud, based on (Chandler 2006)

As seen in Figure 1, each wave consists of a four-stage lifecycle with the final stage of each established wave overlapping with the first stage of the following wave. This places

Cloud at Stage 1, Initiation, a technological discontinuity that is overtaking today's legacy IT architecture. As such, Cloud has created both enthusiasm and apprehension among IT leaders in the US Federal Government. Federal Agencies hear from Cloud providers about significant savings from Cloud. The potential for savings across the US Federal Government is very significant – estimated at $20B annually. (Kundra 2011) Furthermore, Federal IT leaders are obligated to comply with policy from the Federal CIO and the Office of Management and Budget (OMB) as defined in the Federal Cloud Strategy and subsequent OMB guidance. (Kundra 2010) This policy was intended to "accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments." Yet these same IT leaders understand that their Agencies -- as well as the citizens they serve and protect -- depend on their Agency's IT. These are acutely sensitive to the risks involved should they adopt this new Cloud approach without having fully considered all the factors involved in such a decision.

This situation is similar to the opportunities and challenges created by waves of disruptive architectures in the past, such as nTier, Web-based, and Service-Oriented architectures – as well as disruptive technologies, such as: PCs, networking, and internet. IT leaders then and now faced issues surrounding technology adoption. These IT leaders then and now lacked a decision framework to inform their IT decisions on the applicability of the new architectures and technology. To address this shortfall for Cloud, today's IT transformational paradigm, the former Federal CIO proposed a decision framework referred to in this dissertation as the US Federal Cloud Decision Framework

(USFCDF). The USFCDF was part of a larger "Cloud First" overarching strategy. The USFCDF benefited from insights provided by government and industry leaders. But it was immature, lacking further refinement and objective validation. To date, the CIO's initiative has gone largely unused, leaving Federal IT leaders where they were in the past – failing to adopt the new technology in some cases and inappropriately rushing too quickly to embrace it in other cases.

Section One - Cloud

Although the concept of Cloud can be traced to 1961 (Vafopoulos 2007), the term Cloud, and the broader concept of Cloud today was coined only in 1997. (USPTO 1999)

Because Cloud is so new and spans a large portfolio of technologies encompassing several layers of potential services, it has spawned multiple definitions. One set of definitions for Cloud which is gaining greater acceptance globally are those drafted by the US National Institute of Standards and Technology (NIST). (NIST 2011)

NIST defines Cloud computing as "a model for enabling ubiquitous, 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 is composed of:

- Five Essential Characteristics: that describe what is (and is not) Cloud
- Service Models: that describe the value-added level provided by Cloud
- Deployment Models: that describe how the Cloud instantiation incorporates or excludes multiple tenants (customers/users).

This research project adopted NIST definitions and terminology. By adopting these standards to define Cloud, the research project avoided the debate on the semantical question of "what is Cloud." Furthermore, because NIST's definitions are becoming widely accepted globally – for commercial and governments -- and because NIST is part of the US Government, Federal IT leaders are likely to be more accepting of the conclusions of a research project leveraging NIST definitions instead of other academic or non-US definitions of Cloud

Section Two – Federal Government and Cloud

The US Government spans 429 Departments and Agencies (USG 2015) and employs approximately 2.5 million workers. Most of these organizations have specific IT leaders responsible for their IT. These responsibilities span the lifecycle of their IT – advocating funding, defining requirements, formally acquiring IT, sustaining IT, and modernizing their legacy IT. They accomplish this while remaining compliant with guidance and regulations promulgated by other Federal Agencies and Congress. These IT leaders usually lead IT organizations consisting of government personnel and contractor personal so therefore manage a workforce as well. Unlike large corporations with centralized IT departments, the US Government's IT remains considerably decentralized – mirroring the federated organization itself.

It is within this complex context that Federal IT leaders make decisions about their IT capabilities. As new technologies and related IT paradigms emerge, these IT leaders – often independently and in parallel – determine whether to adopt these new capabilities and if so, the best way to proceed. Cloud is one such transformational capability,

consisting of both new technologies as well as a new paradigm for deploying IT capabilities. This section first discusses the nature and scope of IT in the US Federal Government and then overviews the emerging regulations and guidance that affect Federal IT leaders as they consider how Cloud might affect their organization.

Federal Agencies as IT Enterprises

The US Federal Government is the world's largest consumer of information technology, with over 12,930 IT systems costing approximately $80B a year for development, modernization, and sustainment. (OMB 2009). Based on OMB, Cloud offers the potential for $20B in savings each year (Kundra 2011).

One justification for estimating 25% savings is the ability of Cloud to share resources and balance load over more users. Industry has leveraged this Cloud concept to drive savings.

The Senior IT leader within the Federal Government is the CIO. This position was created in 2002 but alternate titles were employed until Vivek Kundra served as Federal CIO (Government 2002). Each Federal agency also has an agency CIO with specific responsibilities and authorities given to the position through Public Law 104-106 in what's now referred to as the Clinger-Cohen Act (Congress 2006). Portfolio management, enterprise architecture, and now Cloud adoption fall under the purview of the agency's CIO.

Federal Guidance on Cloud

Not only does Cloud offer potential benefits in terms of cost savings, agility, and new capabilities, Federal agencies also have received guidance to adopt Cloud. In 2009, the

Federal CIO, through OMB, published the "25 Point Implementation Plan to Reform Information Technology Management." (Kundra 2010) This guidance includes a provision referred to as "Cloud First." This policy was highlighted by Kundra in 2010 and then put into policy by OMB in 2011. Cloud First intended to "accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments." Federal guidance at the time required each Federal agency to jump-start the migration to Cloud technologies by identifying three "must move" services and create a project plan for migration each of them to Cloud solutions and retiring the associated legacy systems. In May 2011, OMB consolidated the "must move" nominations and published a consolidated list of 78 systems Federal Agencies considered for migration to Cloud. (OMB 2011)

Also in 2011, the Federal CIO, through OMB, published the "Federal Cloud Computing Strategy." (OMB 2011) This strategy included a framework for Cloud migration that spanned the lifecycle of a Cloud migration, to include *selecting the systems to migrate*, provisioning the new capability within Cloud services, and then managing the new capability within the Cloud environment. (see Figure 2) This research project focuses on the first phase of that larger Cloud migration framework, which is the "Select" phase that outlines a decision framework for selecting IT systems to migrate. This decision framework is referred to as the US Federal Cloud Decision Framework (USFCDF) and is summarized in the next section.

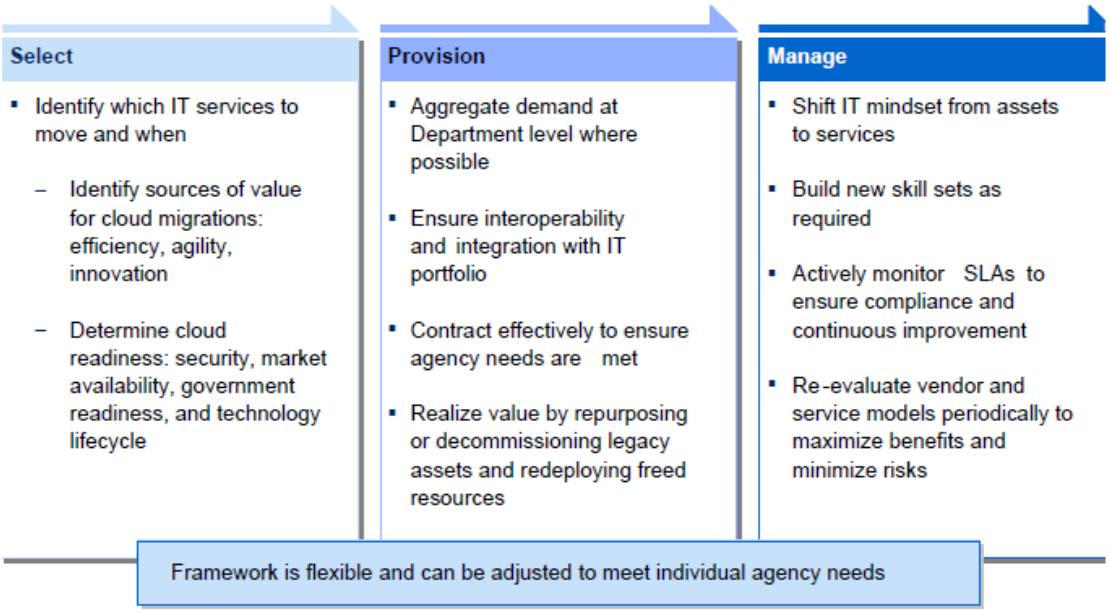


Figure 2 - Kundra Lifecycle Framework for Cloud Migration (Kundra 2011).
This research project focuses on the first block – the selection decision

Section Three – The US Federal Cloud Decision Framework (USFCDF)

For this research project, the USFCDF is the term used to describe the decision framework outlined in the "Select" phase of the larger Cloud migration framework depicted in Figure 2. For this research project, the intent of the USFCDF is to enable Federal IT leaders decide whether a legacy IT systems should migrate to the Cloud. As stated by Kundra, the USFCDF was created to "Provide a decision framework … to support agencies in migrating towards cloud computing." (Kundra 2011) . The USFCDF consists of three primary constructs:

- Nine decision factors (DFs), spanning the issues that need to be evaluated for a decision on migrating to the Cloud.

- The decision structure (DS), a model that relates the overarching aspects of the decision and is used to group or categorize the DFs.
- The decision question (DQ), which is how the migration question itself is formulated for the decision maker.

See Figure 3 for a graphic depiction of these USFCDF constructs.

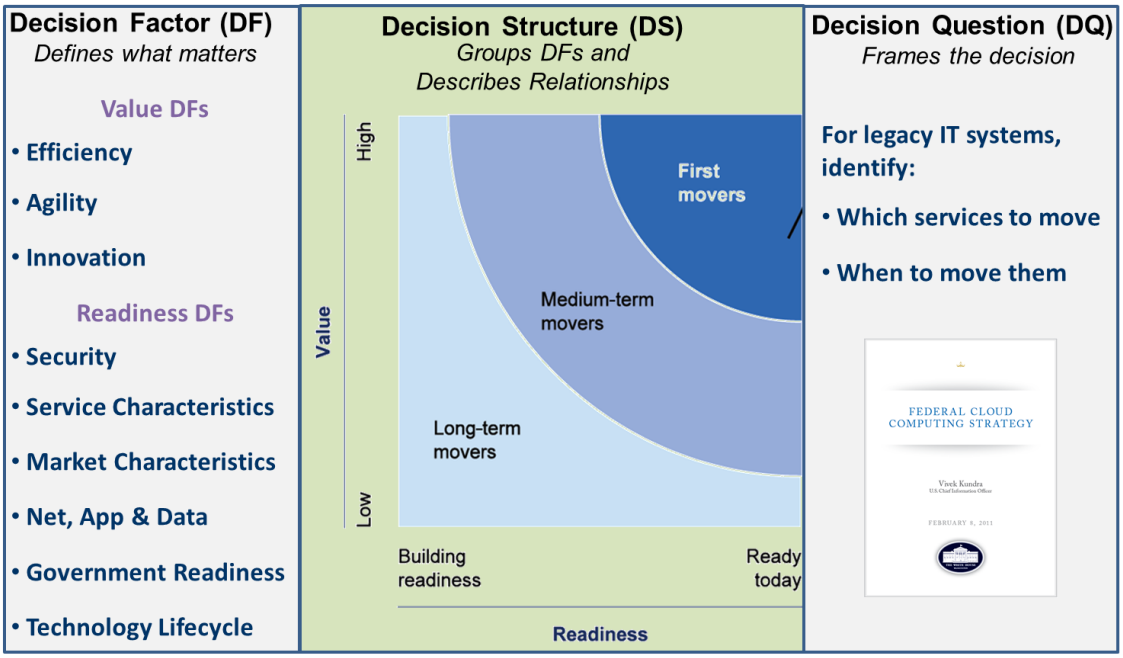


Figure 3 - Three Constructs of the US Federal Cloud Decision Framework (USFCDF)

Section Four – Problem Statement

As noted earlier, Federal Agencies spend $80B annually developing, modifying, and sustaining over 12,000 IT systems using traditional (non-Cloud) IT methods. (OMB 2009) Because of these costs – as well as the reliance the US Government places on these systems – the Federal CIO directed Federal Agencies to pursue a "Cloud First"

policy for adopting Cloud. Yet, Federal Agencies have designated relatively few Federal IT systems to migrate to the Cloud. Also, Congress and the General Accountability Office have questioned the basis of at least one of those migration decisions. The problem, summarized in one sentence is as follows: *Federal Agencies lack a common, validated decision framework for deciding whether a legacy IT system should migrate to the Cloud.*

Section Five – Research Methodology

To investigate Federal Cloud decision frameworks, the researcher moved beyond prior work (which had been primarily surveys) to investigate actual Cloud migration decisions by US Federal Agencies. This research project investigated several recent decisions about migrating Federal email systems to the Cloud to determine whether the USFCDF is suitable as the basis for a common Cloud migration decision framework across all Federal Agencies.

Multiple Case Study and Wigmore Inference Modeling

The researcher applied the multi-case study methodology based on Robert Yin (Yin 2012) and further informed by Robert Stake (Stake 2006), arguably the two leading experts in case study research and whose texts are employed in related courses taught at George Mason University.

The methodology incorporated the Federal CIO's decision framework (the USFCDF) as the theory (Yin's term) for the cases researched. The USFCDF provided a common lens for the comparative analysis of the disparate cases – a research "Rosetta Stone." Figure 4 depicts graphically how the USFCDF, developed by former Federal CIO Vivek Kundra,

serves to map the decision elements found in each case onto a common set of decision factors.

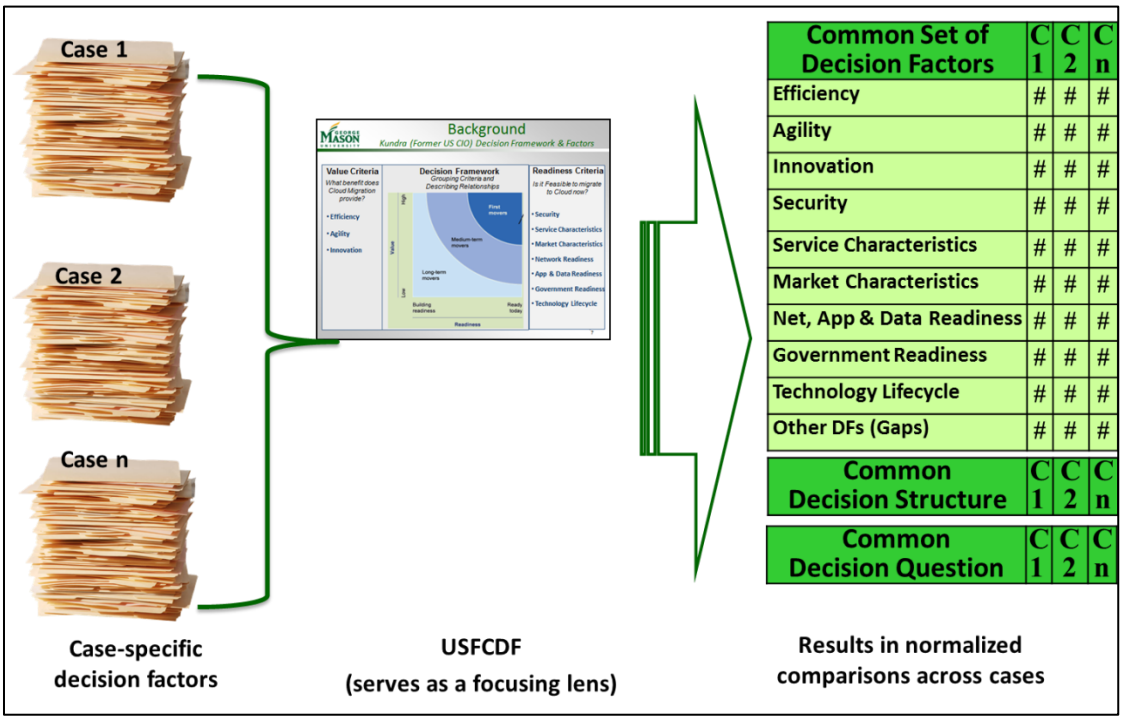


Figure 4 - Incorporating Federal CIO (Kundra's) Cloud Decision Model in the Research Methodology.

The researcher methodology also incorporated standards and models related to Cloud as described by the US National Institute of Standards and Technology (NIST). By adopting the NIST definitions of Cloud, the research benefited from a consistent taxonomy and terminology related to Cloud. This adoption obviates the potential conceptual variances that otherwise might be introduced from differing personal interpretations of Cloud. For this research project Cloud means what NIST says Cloud means. Finally, the researcher marshalled the evidence from the case studies into a

Wigmore inference model (Kadane 1996), linking the case study observations to the hypothesis through the use of Araucaria, a software tool for argument analysis, diagramming, and representation developed by the Division of Applied Computing, University of Dundee. (Reed 2004)

Research Questions

To address the problem described earlier in Section Four – Problem Statement, the researcher sought to answer the five research questions and associated sub-questions as seen in Table 1.

Table 1 - Research Questions

Questions & Sub-questions
1. Do the USFCDF decision factors provide value to Federal IT leaders deciding whether a legacy IT systems should migrate to the Cloud?
a. Are all USFCDF decision factors necessary?
b. Is the set of USFCDF decision factors sufficient?
2. Does the USFCDF decision structure provide value to Federal IT leaders deciding whether a legacy IT systems should migrate to the Cloud?
a. Does a decision structure (in general) provide value?
b. Is the Value-Readiness paradigm of the USFCDF decision structure useful for marshalling decision factors?
3. Does the USFCDF decision question provide value to Federal IT leaders deciding whether a legacy IT systems should migrate to the Cloud?
a. Is the USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions?
b. Is the USFCDF decision question consistent with the needs of the decision maker?
4. Is email a well-defined legacy IT system?
a. Are email systems in the Federal defined by a small set of similar legacy commercial products?
b. Is email used across the Federal enterprise?
5. Would Cloud migration decision-makers have benefited from prior-knowledge of a validated USFCDF?

Questions 1, 2, & 3 align directly with the hypothesis and the sub-hypothesis described later in this section. Question 4 relates to whether the results of the research can be generalized beyond Email to the larger set of well-defined legacy IT systems. Question 5 relates to the value of solving the research problem.

Purpose of the study

The purpose of the study is to further knowledge of, and potentially provide a solution to the problem regarding a Federal agency's ability to decide whether a particular IT system should be migrated to Cloud.

Through research actions, the study will also provide greater clarification on the meaning and measures of the decision factors as they relate to the Cloud IT decision. This should transform Kundra's model from a concept to a usable framework.

Anticipated Findings and Resultant Hypothesis

Prior work, to include recent surveys of commercial and federal IT leaders, informs this research project and provides insights into anticipated findings. The researcher anticipated that the USFCDF, with a slight evolution, can provide value to Federal IT decision makers in determining whether a well-defined legacy IT system should migrate to the Cloud. In particular, the researcher anticipated that a Federal IT leader would find each of the three elements of the USFCDF of value to include:

- The decision factors
- The decision structure, and
- The decision question

The researcher also anticipated that the Federal Agencies will consider email an example of the larger class of well-defined legacy systems.

The research hypothesis is formed around the anticipated findings. Specifically, the research hypothesizes the following:

Hypothesis: *The US Federal Cloud Decision Framework (USFCDF) provides value to Federal IT decision makers in determining whether a well-defined legacy IT system should migrate to the Cloud.*

Sub-hypothesis 1*: The USFCDF decision factors provide value to the Federal IT decision maker*

Sub-hypothesis 2*: The USFCDF decision structure provides value to the Federal IT decision maker*

Sub-hypothesis 3*: The USFCDF decision question is consistent with the needs of decision maker*

Each of the three sub-hypotheses is further broken down into a pair of subsub-hypothesis as discussed in Chapter 3. This provides six nodes at the lowest level of the Wigmore inference diagram, enabling more granular mapping of case study evidence to the hypothesis.

Section Six – Research Contributions

This research contributes to the body of knowledge in several ways. For Cloud and Information technology, it extends prior research – primarily opinion surveys – to observations from actual Cloud migration decisions. In addition to gaining insights from actual cases, this research project will also extend the research in Federal Cloud migration from a partial set of decision factors concerned primarily about the feasibility and risk of Cloud to a broader set of decision factors found in the USFCDF. Beyond decision factors, this research will explore the decision structure and decision question and address aspects of the cloud migration decision question missing from prior research.

This research project should also contribute to the body of knowledge pertaining to two trends in systems engineering – services engineering, and systems of systems. Cloud is a service, as noted by NIST listing the Cloud Service Models. Services engineering has become increasingly important to DoD IT. For example, DoD expanded the traditional systems architectural frameworks to incorporate services in the latest revision of the Department of Defense Architecture Framework (DoDAF). Another systems engineering aspect of Cloud is that it exhibits attributes of a system of systems – for example, NISTS Hybrid Cloud deployment model, which represents a growing body of study within DoD and systems engineering.

In addition to extending the body of knowledge about Cloud and systems engineering, the results of the research project should create actionable contributions benefiting Federal IT leaders. In the near term, the results of the research project should provide the US Federal Government the insights and validation to adopt a common Cloud migration decision framework. That, in turn should enable better decisions, which one could argue would lead to better results in terms of increased benefits to citizens at reduced governmental costs. Two researchers at MIT reported evidence that good technology governance improves performances of organizations (McAfee 2011).

Section Seven – Overview of Contents

The remainder of this paper is organized as follows:

Chapter 2 – Review of literature. Special emphasis on: Cloud; Federal Government IT; Decision frameworks and factors; and Systems engineering.

Chapter 3 – Research Methodology. Outlines the rationale for applying a multicase study (aka multiple-case study) methodology for this research project. Having adopted the multicase methodology, this chapter then details the specifics of this research project using the six-step multicase study construct – i.e. research plan – outlined by Robert Yin and further informed by Robert Stake. Chapter 3 also describes the Wigmore inference model and the Araucaria modeling tool.

Chapter 4 – Case study summaries. This chapter summarizes the findings of each of the five cases. Three full case studies investigated all five research questions. Two partial case studies provide additional insight to account for specific research areas that were intentionally varied (not kept as research constants) for the research project. Background for each of the five cases can be found in the appendices.

Chapter 5 - Synthesis of Multiple Case Study Findings. Analysis of the observational evidence from the case studies and relating these findings to support the hypothesis applying Wigmore inference diagrams and leveraging the Araucaria inference diagramming tool.

Chapter 6 – Conclusions. Summarizes the strength of the evidence and inferences supporting the hypothesis, describes the value of the results, and suggests further areas of research.

2. REVIEW OF LITERATURE

The concept of utility computing predates the wide adoption of the term Cloud Computing. In 1961, John McCarthy was the first to publicly suggest, based on the emerging timeshare computer model, that computing could someday be considered like a utility. McCarthy declared at MIT's Centennial that "If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility. The computer utility could become the basis of a new and important industry." (Vafopoulos 2007)

The term "Cloud" was not applied to McCarthy's utility concept until the late 1990's. It's generally accepted that the term was first coined by Netcentric Corporation in 1997 as they filed a trademark request, which they later abandoned. (USPTO 1999) However, the term did not come into general usage for another 10 years after the trademark request.

The Federal Government's use of cloud-like utility computing predates the wide adoption of the term Cloud also. For example, the Defense Information Systems Agency (DISA) discussed procurement of several IT services in 2006 without mentioning the term Cloud. One such service discussed was the Global Information Grid (GIG) Content Delivery Service (GCDS). (DISA 2007) Today, DISA lists GCDS under its catalog of Cloud offerings it provides to other Federal agencies. (DISA 2011)

Because Cloud is relatively new and increasingly popular, the term is often applied to IT systems that others might argue are not actually Cloud. For example, the list of 78 Federal Cloud initiatives in 2011 included examples of an agency's web-enabling legacy systems and claimed that such enhancements represented a Cloud implementation. (OMB 2011) However, one can't presume these Federal agencies disingenuous because the 78 case studies were collected without the Agencies having first received guidance on what defined a Cloud implementation. Definitions of Cloud proliferate. Gartner noted that "The term "Cloud computing" is being loosely applied and defined differently -- and it's "creating a lot of confusion in the market." (Gartner 2008) Yet even Gartner posted (and later changed) its own definition of Cloud, further adding to the confusion in the marketplace. Gartner now defines Cloud Computing "as a style of computing where scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies. First and foremost is the concept of delivering services (i.e., delivering results as opposed to IT components). (Gartner 2011) Forrester and others have also advocated their own definitions of Cloud.

This research paper focuses on Cloud in the Federal Government. Therefore, it would be most appropriate to adopt a Federal definition of Cloud. The National Institute of Standards and Technology (NIST), provides such a definition; "Cloud computing is a model for enabling ubiquitous, 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." (NIST 2011) This definition and the associated

characteristics of Cloud, are becoming widely accepted by the US Federal Government. For example, the US Army incorporated NIST definitions of Cloud when they solicited feedback from industry about the Army email migration to Cloud. (Olson 2009) A growing number of other governmental, commercial, nonprofit, and academic organizations globally are also adopting the US-initiated NIST definitions. (Alliance 2009) Therefore, unless otherwise noted, when Cloud is discussed for this research project, the researcher presumes the NIST definitions of Cloud.

Section One – Cloud Characteristics

This section describes in more detail what Cloud is and what differentiates it from other IT concepts by analyzing the characteristics of Cloud.

Cloud has five defining characteristics as depicted in Figure 5. (NIST 2011)

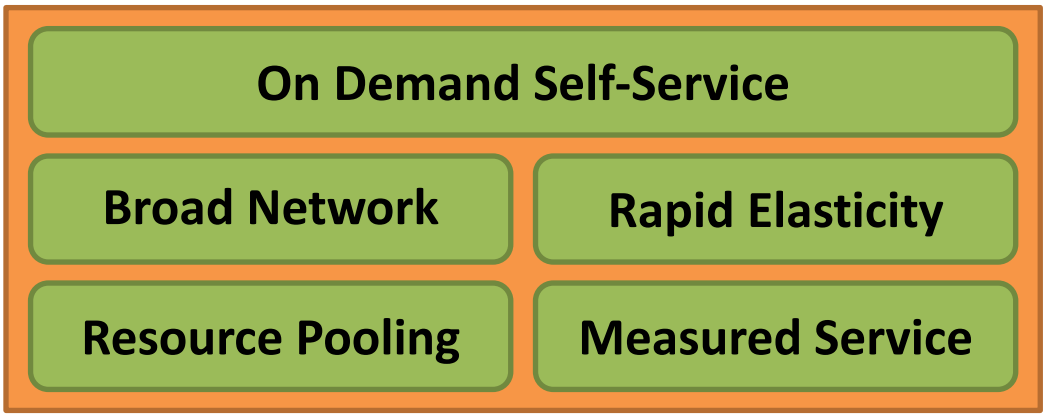


Figure 5 - Cloud Characteristics (NIST 2011)

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. (NIST 2011)

Underlying this concept is that provisioning, which is the act of making IT resources available and usable (physical or virtual), can not only be requested by a user, but also be implemented directly through automated systems based on the user's request. Furthermore, these requests can happen at the time desired by the user, and not just at some predetermined schedule of times, such as the technology refresh for a system. Web developers have been familiar with this characteristic of Cloud since the late 1990's when web hosting firms provided web developers the ability to sign up for a hosted web server by completing web-based forms and paying for the service on-line.

Broad Network Access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs. (NIST 2011)

Although some users may care where their Cloud service originates because of security or political concerns, in general this Cloud characteristic abstracts the location of the data and associated processing. Also implied by this characteristic is that the Cloud service is only loosely coupled with the devices used to access the service, enabling access through multiple devices.

Note that the NIST definition implies by nature of the devices listed that the Cloud service consumer is a human user. However, with increasing need for machine-to-

machine connections, Cloud services will also need to interact with other Cloud and non-Cloud IT systems.

Within the Federal government, some Cloud Services either exist, or are being developed to support other applications or Cloud services. A good example of this is a security service to manage Public Key Encryption. (OMB 2011) This Cloud service would enable other Cloud services to authenticate users in a consistent fashion without having to develop a security function for each user-facing Cloud service.

Broad network access is assumed by many organizations and individuals, particularly those who work in offices supported by robust internet connections as well as those with mobile devices in areas covered by mobile carriers. For some Federal agencies however, broad network access is not assured or even likely. For example, first responders deploying in the aftermath of hurricane Katrina had limited connectivity individually and within their mobile command centers. Also, within the Department of Defense (DoD), military members must often deploy to austere locations far from US-based datacenters and rely on devices that may not interoperate with host nation telecommunications. In fact, availability is the top concern among those surveyed within DoD. (Killaly 2011)

Resource Pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of

abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. (NIST 2011)

Resource pooling – and its complement, multi-tenancy – are the primary drivers for the cost savings of Cloud. For example, Ted Alfred and Gwen Morton of Booze | Allen | Hamilton concluded from their research that the servers in the Federal Government operate at an average of 12% utilization, (Morton 2009) indicating significant value in pooling processing capability among multiple Cloud service consumers.

Servers are more easily shared today because virtualization technology enables a single server to appear as multiple virtual servers to the service consumers. Virtualization is an example of relatively new technologies that, through Cloud services, enable resource pooling and in turn, provide the opportunity for savings from Cloud migration.

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. (NIST 2011)

The term "rapid," although not quantified in units of time, denotes a pace faster than a deliberate physical stand-up or expansion effort using dedicated resources.

Another key aspect of rapid elasticity is that the Cloud services consumer can rapidly release Cloud resources, freeing them for other uses or users and, with most Cloud service providers' business model, reduce expenditures. An example of this elasticity in the Federal Government is the community Cloud named Nebula which is deployed by the

National Aeronautics and Space Administration (NASA). Nebula supports NASA for public education, mission support, data communications, and storage. In the dates leading up to LCROSS mission culmination (the impact on the moon in search of water on the moon), Nebula enabled support for a surge of data and a subsequent end of data (the impact). (West 2010) Another example of a surge in IT needs for a Federal agency did not turn out as well. During the Cash Allowance Rebate System (aka "Cash for Clunkers"), the Federal Government deployed a traditional IT system. When demand surged, the system initially crashed under the load and did not meet demand levels fully for 30 days. (Kundra 2010-2) Furthermore, when the program ended, the Federal Government still owned the hardware and software for a system no longer needed.

Measured Service

Cloud systems automatically control and optimize resource use by leveraging a metering capability[1] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. (NIST 2011)

This final characteristic of Cloud, measured service, prompts comparison of Cloud to utilities such as electricity and water. A Federal agency consuming computing power pays for the services it consumes, but need not purchase the equivalent of a generator or well in advance in order to obtain these services.

Section Two – Cloud Service Delivery Models

Cloud services are categorized according to the nature of the Cloud service provided by a Cloud service provider, or conversely, acquired by a Cloud service consumer. The three layers of services defined by NIST (NIST 2011). Figure 6 graphically describes the three Cloud service delivery models.

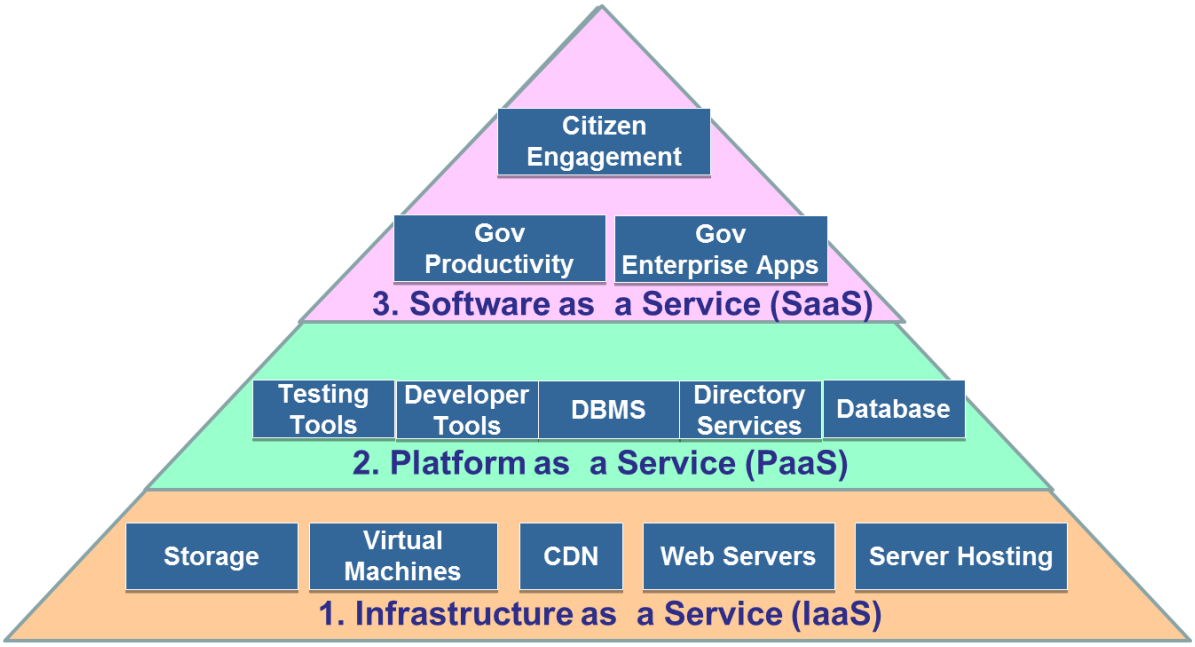


Figure 6 - Cloud Delivery Models (Mink 2011) based on NIST definitions (NIST 2011)

The Cloud Security Alliance (CSA), an international body focused on Cloud security and privacy, published an expanded version of the NIST model. CSA adopted the NIST service delivery model and added additional granularity to better define which functions belonged within each delivery layer. According to CSA, "Understanding the relationships and dependencies between Cloud Computing service delivery models is

critical to understanding Cloud Computing security risks." (Alliance 2009) The adoption of the NIST model by this international organization, which is focused on the critical issue of Cloud security, indicates that the NIST framework has gained credible and broad acceptance beyond the US Federal Government.

Infrastructure as a Service (IaaS - Level 1)

IaaS provisions processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). (NIST 2011)

IaaS typically includes the lower-level services, such as virtual servers, storage, and web servers. IaaS may also provide a Cloud Delivery Network (CDN) which networks servers together and stages content closer to end users.

Within The Federal Government, the most notable deployment of IaaS is DISA's Rapid Access Computing Environment (RACE). According to DISA, RACE provides virtual servers provisioned through a self-service web portal. (DISA 2011) RACE provides test and development virtual servers available for use by the next business day, and the follow-on comparable production servers available within 72 hours. The standard package includes a Central Processing Unit (CPU), one (1) GB memory, 60 GB disk storage, and Internet Information Services (IIS) for Windows-based servers or LAMP (Linux, Apache, MySQL and PHP) for Red Hat servers. Variable server configurations of

one to four (1-4) CPUs and one to eight (1-8) GB of memory are available. DISA provides IaaS through infrastructure hosted at its Distributed Enterprise Computing Environments (DECCs).

Another example of IaaS in a Federal agency is the planned Cloud for the Federal Aviation Administration. FAA selected a hardware and software suite from HP Inc., repurposed the former FAA Command Center in Herndon, Virginia for the hosting facility, and is the midst of selecting a systems integrator to build the IaaS Cloud in that facilities using the HP hardware and software. FAA intends to not only use the FAA Cloud for their own use, but also to resell it to other Agencies. According to their lead for this initiative, FAA will target smaller Federal agencies, offering the Agencies Cloud services that would be impractical for them to develop themselves, but still with the affordability and related security provided by a fellow Federal agency. (Mink 2011-2)

However, IaaS provided by a Federal agency has limitations. As noted by former DoD C3I Paul Strassmann, (the position that later became the DoD CIO) in his BLOG comments about DISA's RACE, "Before DoD proceeds with the placement of its run-time operations with diverse IaaS vendors, DISA must see to it that standards are in place that will assure interoperability and compatibility across proprietary solutions offered by competing IaaS vendors such as Oracle, which supports only Oracle specific IaaS." (Strassmann 2011)

Platform as a Service (PaaS - Level 2).

Deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does

not manage or control the underlying Cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. (NIST 2011)

PaaS builds upon IaaS to provide the user middleware. This middleware often includes developer tools; testing tools; databases and associated database management systems, and directory services.

Within the Federal Government, one of the most visible PaaS clouds is DISA's Forge.mil. This services offers application life-cycle management (ALM) software-development tools, such as version control, bug tracking, requirements management, and release packaging, along with collaboration tools such as wikis, discussion forums, and document repositories to enable collaborative development among geographically distributed teams. Rob Vietmeyer, DISA's project manager for Forge.mil claims that "once a customer agrees to the standard support agreement and provides the required funding for this service, project space can be made available within hours. Benefits to the program include: (a) lower total cost of ownership; (b) faster start-up time (hours versus months) and reduced cost; (c) delivery and storage of software assets within reliable government-owned software repository; and (d) support for collaboration among geographically dispersed teams." (Vietmeyer 2011)

Forge.mil offers two levels of service, SoftwareForge and ProjectForge. SoftwareForge is available at no charge for authorized users and provides basic capabilities with limited flexibility. ProjectForge permits customers, for a fee, to restrict read and write access to each project through a fine-grained management of permissions.

An analysis of Federal Cloud initiatives shows that PaaS is the most popular of the three NIST-defined delivery models. See Figure 7. Examination of the 78 Federal Cloud initiatives shows a strong number of them using PaaS as a platform for software development, leveraging the elasticity of Cloud to quickly stand up the develop environment and then discard it (de-provision it) after development is complete. The other high use of PaaS is for Website hosting. Websites leverage a fairly standard set of web-hosting middleware, making them ideal candidates to leverage the additional capabilities PaaS offers over IaaS while also retaining the flexibility often not possible in SaaS.

The distribution of IaaS, PaaS, and SaaS depicted in Figure 7 is somewhat in contrast to the distribution of Cloud service levels as measured globally in dollars.

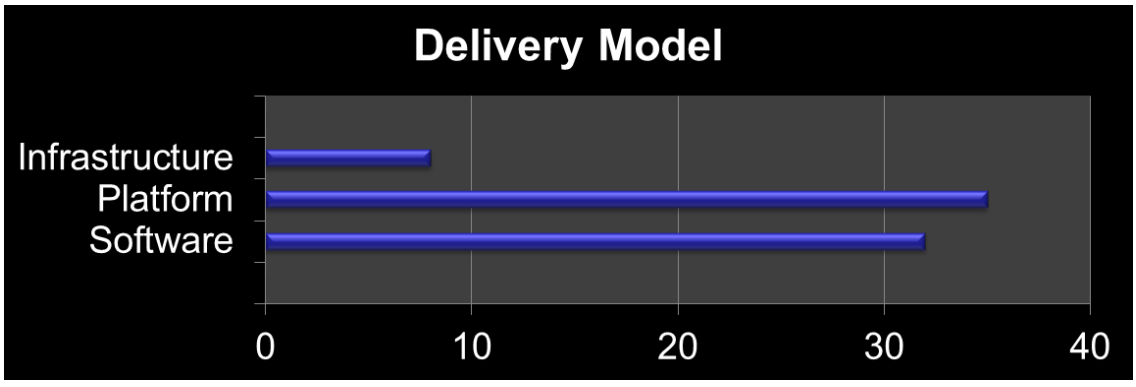


Figure 7 - Analysis of 78 self-report Cloud initiatives (Mink 2011) from data reported by OMB (OMB 2011)

According to IDC, world-wide public IT Cloud services outlays in 2009 totaled $16.5 billion and fell into the following categories and percentages of total spend: (Plant 2011)

- Applications (49%)
- Application development/deployment (10%)
- Infrastructure software (20%)
- Servers (12%)
- Storage (9%)

By aligning the three NIST-defined service delivery models with IDC's five spending categories, IDC's survey could be generalized to indicate that worldwide Cloud spending is allocated as follows: IaaS (Servers & Storage & Infrastructure Software) 41%, PaaS (Application development/deployment) 10%, and SaaS (Applications) 49%.

Software as a Service (SaaS - Level 3)

Provider's applications running on a Cloud infrastructure. The applications are accessible from various client devices are through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (NIST 2011)

SaaS is the type of Cloud service most familiar to the average person, particularly those without IT backgrounds. Examples of SaaS include Google's Gmail and Facebook, as well as other utility-type services users would not quickly associate with traditional Cloud discussions, such as a mobile phone's text messaging service. SaaS, the highest of NIST's three defined service delivery models, allows a user with an access device and

network connectivity to use software without having to own or maintain the software and the underlying infrastructure.

One of the largest and longest-running examples of SaaS in the Federal government is Defense Connect Online (DCO), a Cloud service hosted by DISA and used by numerous other Federal organizations. Over 400,000 government users have subscribed to DCO and in March 2011, consumed nearly 30 million minutes of service. (DISA 2011) See Table 2.

Table 2 - Number of DCO users. (DISA 2011)

Organization	**# of users**
AFRICOM	2,982
CENTCOM	5,744
DISA	13,096
EUCOM	6,894
JFCOM	7,016
NORTHCOM	16,406
PACOM	12,357
SOCOM	3,552
SOUTHCOM	4,931
STRATCOM	3,503
TRANSCOM	2,418
USA	77,031
USAF	106,442
USMC	14,287
USN	61,887
Undisclosed	61,454+
TOTAL	400,000+

Among the 78 Cloud initiatives in the Federal Government reported to OMB, the most common use of Cloud overall is for website hosting, but for PaaS, the most common use is for email. See Figure 8.

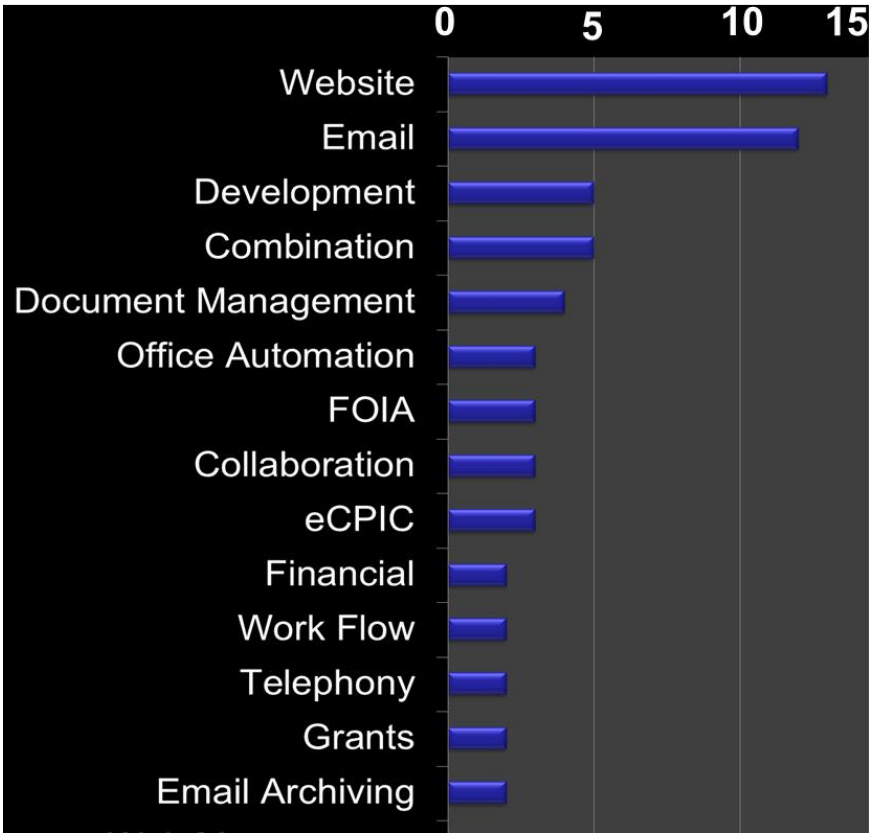


Figure 8 - Analysis of 78 Federal Cloud candidates by function[1]. (Mink 2011) from OMB data (OMB 2011)

The most ambitious deployment of email, and therefore likely to be the largest SaaS deployment in the Federal Government, is DoD Enterprise Email. On October 25, 2010,

[1] Excludes functions with fewer than two Federal examples.

the US Army along with DISA announced agreement on enterprise email. (Army 2010) This Cloud service would use Microsoft Exchange as the back end (enterprise application) and be accessible via the network for webmail and for support to email clients such as Microsoft Outlook. Enterprise email plans to serve over 1.4 million unclassified network users and 200,000 secret network users from the Army, US Transportation Command, US European Command, and US African Command, and had originally targeted completion by September 30, 2011. (Army 2010)

DoD believes this effort will produce significant generate annual savings exceeding $100 million per year in FY13 and beyond. Army IT experts also believes enterprise email will provide better service than their legacy email systems. "The Army's move to Enterprise Email enables users to access their Army email from any DoD location and to collaborate with any Army user worldwide via a Global Address List and enterprise calendar sharing," said Lt. Gen. Jeff Sorenson, the Army Chief Information Officer/G-6. (Army 2010)

But by mid-August 2011, enterprise email had only 8,900 users (Hale 2011). According to John Hale, Program Manager for Enterprise Email, enterprise email deployment was halted temporarily until DISA and Army could work through problems with other related enterprise infrastructure, particularly the Army's network and desktops. The Army's infrastructure could not support this enterprise email service.

Facilities as a Service (FaaS - Level 0)

NIST defined the three delivery models described above: IaaS, PaaS, and SaaS. However, literature studies and exploratory interviews with Federal IT leaders indicate

two other layers of Cloud-like services either employed or under consideration. Although not formally titled nor sanctioned by a standards body today, the following two titles characterize these two additional delivery models: Facilities as a Service (FaaS) and Activity as a Service (AaaS). See Figure 9 for combined relationships of the five delivery services.

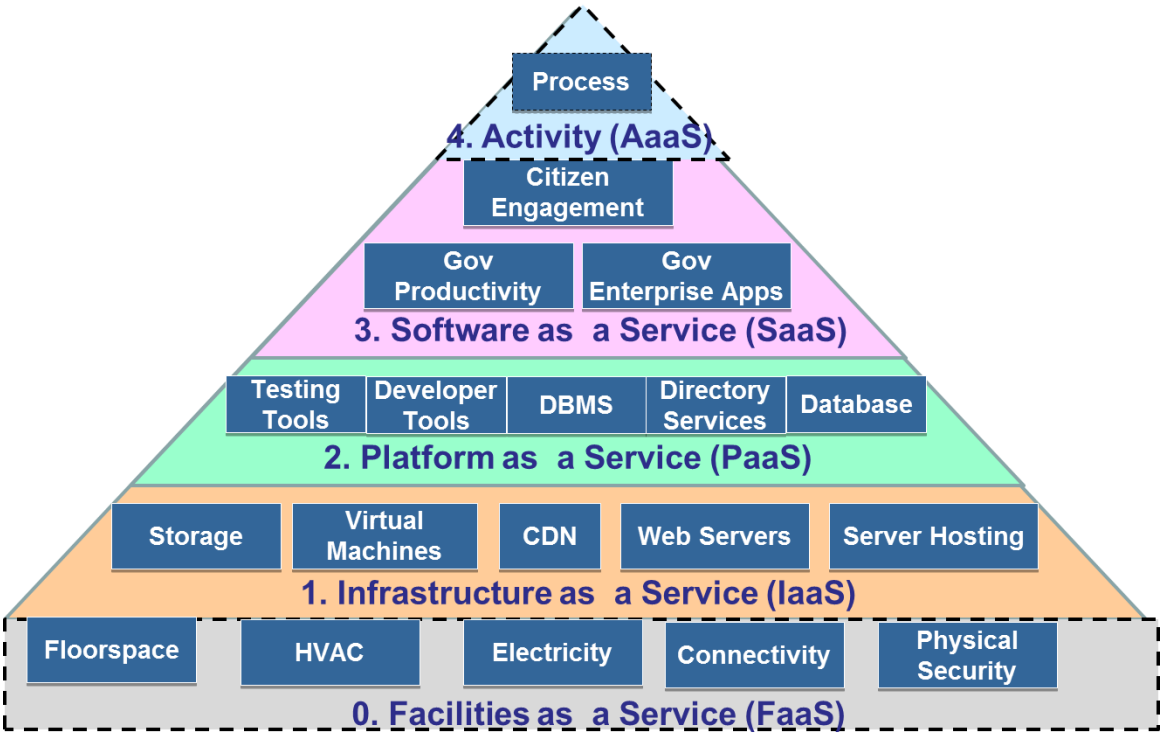


Figure 9 - Expanded view of Delivery Model

FaaS, as proposed in the figure above as a service layer foundational to IaaS, provisions floor space, electricity, connectivity and other fundamental facility hosting resources where the consumer is able to deploy and run arbitrary systems, which can include their own servers, storage, and other components of IaaS, PaaS, and SaaS. The consumer

does not manage or control the underlying facility infrastructure but has physical access and control over the equipment hosted at the facility.

There are many examples of FaaS being applied, or planned within the Federal Government. In one example, The Veterans Administration (VA) is exploring FaaS provided by DISA to host the VA's Veterans Information System and Technology Architecture (VistA), an enterprise-wide electronic health record system (Simpson 2011). This FaaS involves 10,000 square feet of floor space, electrical power, network connectivity, and physical security at the DECC entrance.

The FAA plans its own FaaS to complement their emerging IaaS offering. They will use their legacy FAA Command Center in Herndon, Virginia. FAA is targeting FaaS for their own use as well as for other small Federal agencies. FAA hopes that once other agencies get comfortable with their FaaS offering, they will then become more likely to move up to IaaS. (Mink 2011-2)

Activities as a Service (AaaS - Level 4)

Activities as a Service is another Cloud-like service delivery level seen in the Federal Government, but not (yet?) incorporated into NIST's three-tier set of delivery services. This top layer of service delivery that could be described as either Processes as a Service (PaaS) or Activity as a Service (AaaS). Because the acronym PaaS has already been reserved for Platform as a Service, this observed top layer of services will be referred to as AaaS.

Like the service delivery layers below it, AaaS abstracts services from the user and consumer. In the case of process activities, the user no longer need interact with software

except for actions initiating a process and later resolving interim issues. In general AaaS outsources an activity instead of doing the activity in house using legacy or cloud-based IT services. For example, instead of using a SaaS service like Monstor.com to identify and track candidates in support of internal recruiting activities to onboard new government talent, a Federal Agency may simply outsource the recruiting activity itself. The rationale to include FaaS and AaaS in this paper is to provide a consistent continuum of Cloud-like service delivery layers for Federal decisions migrating activities and their associated systems to an external service provider. This would allow all five layers to be discussed and considered within the same decision framework and factors this paper suggests for the three NIST-define service delivery layers. This approach resonated with the IT leadership of FAA managing their upcoming IaaS offering. (Hale 2011)

Section Three – Cloud Deployment Models

Cloud deployment models describe how a Cloud service may be shared with other organizations and users. Cloud derives much of its value through multi-tenancy. Yet other factors, such as the need to segregate data for protection on one hand, or the need to co-locate data for complex analysis on the other hand requires the definition of several deployment models. NIST organized Cloud deployment into four models. (NIST 2011) Figure 9 graphically depicts the relationships of these four Cloud deployment models.

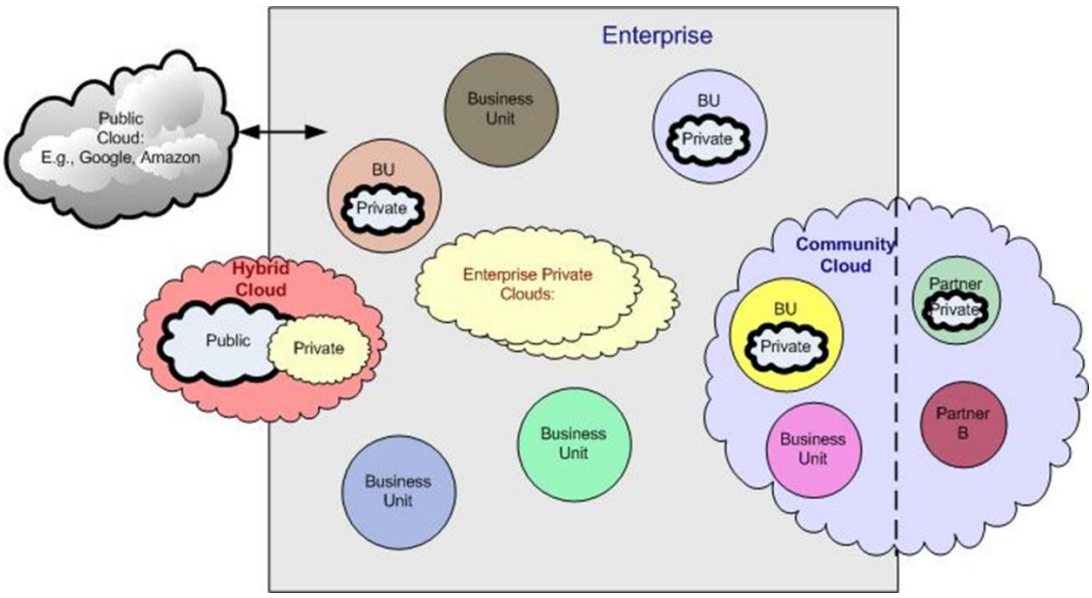


Figure 10 - Cloud Deployment Models (Graphic courtesy of Victor Brown, StrategicIT.com)

NIST provides the following definitions of these four deployment models:

Private Cloud. The Cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community Cloud. The Cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public Cloud. The Cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government

organization, or some combination of them. It exists on the premises of the Cloud provider.

Hybrid Cloud. The Cloud infrastructure is a composition of two or more distinct Cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., Cloud bursting for load balancing between clouds).

Little data has been discovered to quantify the use of models employed or planned across the Federal space. For example, OMB reported 78 IT capabilities that have moved, or are moving to Cloud. Yet, this data did not specifically identify the deployment model nor did it contain sufficient information to deduce the deployment model of many of those 78 systems. See Figure 11 below.

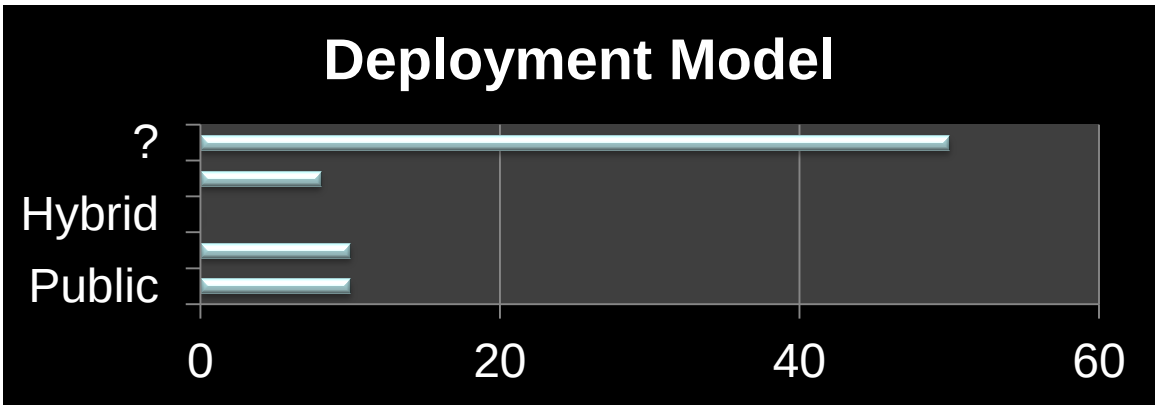


Figure 11 - Deployment models for Federal 78 Cloud initiatives. (Mink 2011) from OMB data (OMB 2011)

Another approach for analyzing deployment models in the Federal Government is to identify Cloud service providers within the Federal Government. By definition, this

approach would not include any public Cloud deployment model offerings -- public Cloud is totally external to a Table 3 summarizes the major Federal Cloud providers with their associated service delivery and deployment models.

Table 3 - Service Delivery and Deployment Models of major Federal Cloud providers

Provider	Cloud Service	Delivery Model	Deployment Model
GSA (GSA 2011)	Cloud IT Services	SaaS PaaS IaaS	Community
DISA (DISA 2011)	Rapid Access Computing Environment (RACE)	IaaS	Community
DISA (Vietmeyer 2011)	Forge.mil	PaaS	Community
DISA (DISA 2011)	Defense Connect Online (DCO)	SaaS	Community
DISA (Army 2010)	Enterprise Email	SaaS	Community
FAA (Mink 2011-2)	Infrastructure Services	IaaS	Community

Although these six Cloud offerings vary in their delivery model, they all conform to the definition of a community deployment model. By adopting a community deployment model, these Federal Cloud offerings reflect a middle position, trading off some of the perceived security of a private Cloud (which by definition would be used only by the owning organization), while gaining economies of scale by including trusted partners – in this case, other Federal agencies.

The four NIST-defined deployment models often raise questions about the relationship between trust and other deployment model attributes such as ownership, management, & physical location. Table 4 below helps depict these relationships.

Table 4 - Relationships among Cloud deployment models (Alliance 2009)

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization / Third Party Provider	Organization / Third Party Provider	On-Premise / Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

Section Five – Cloud Providers and Cloud Enabling Technologies

As noted earlier, utility computing was first publically described by John McCarthy in 1961. Why did it take fifty years for Cloud to become feasible? Winans and Brown attempt to answer this question as part of their examination of architectural approaches for Cloud. (Winans 2009) They posit that the current context versus that of the recent past is "qualitatively different." They drew their conclusion by researching the evolution and current state of technical capabilities such as broadband, storage, memory, operating systems, XML accelerators, virtualization, and other relatively recent innovations.

New firms and new technologies emerge frequently, so it's not feasible to create an exhaustive and authoritative snapshot of Cloud-related firms. However, organizations such as OpenCrowd have assembled a list of firms categorized into four groups. (OpenCrowd 2010) Three of the groups align with the NIST Cloud Delivery Model – IaaS, PaaS, and SaaS. These are customer-facing firms and offerings for primarily public Cloud deployments. The fourth category, "Cloud Software" is a sampling of those technologies used by three groups of Cloud providers to execute their Cloud offerings (see Figure 12). Notably missing from this list are traditional enterprise software providers and products, such as Microsoft Exchange, who are repositioning their products for Cloud and subsequently getting traction for private and community clouds.

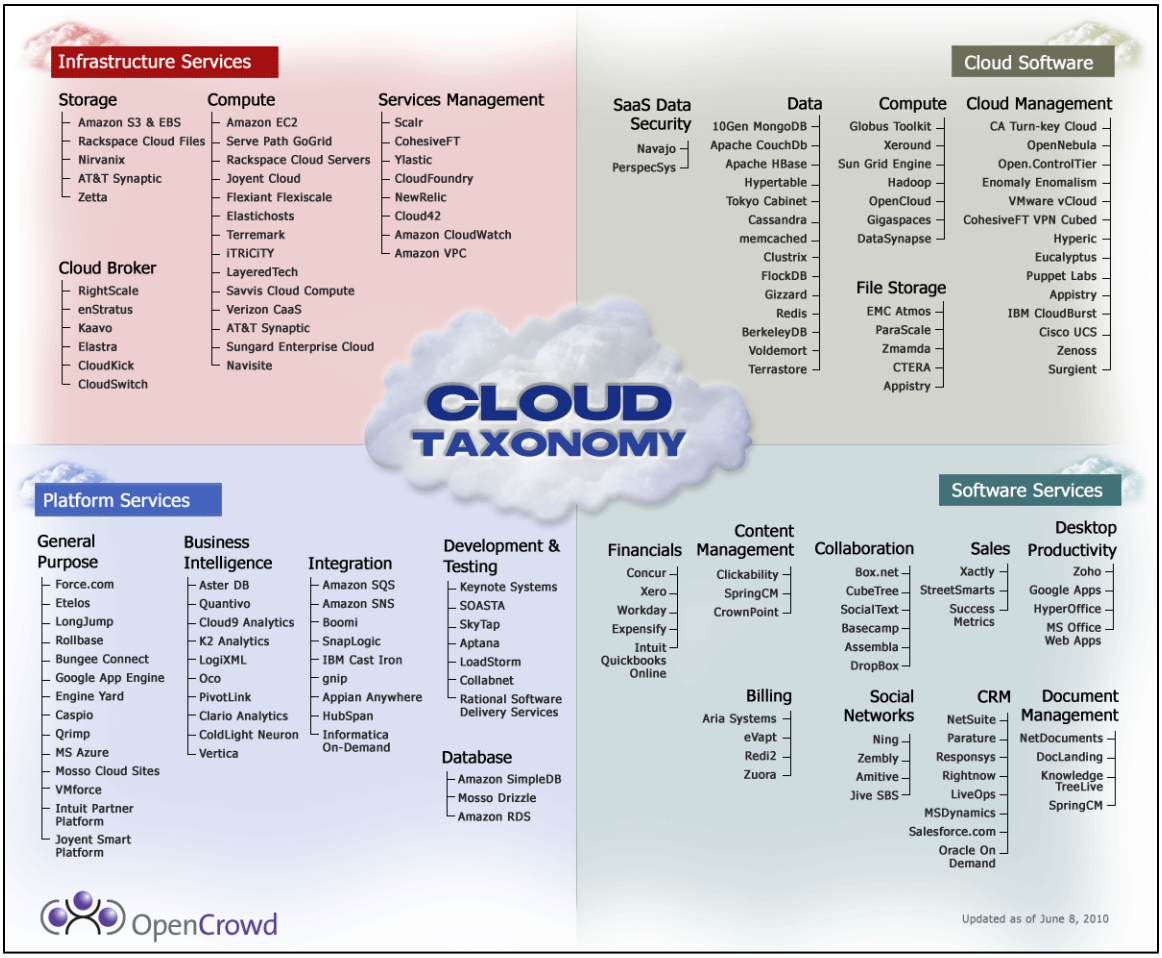


Figure 12 - Cloud Taxonomy of Cloud-related firms and technologies

Cloud providers have been aware of the trend in technology and have invested in infrastructure to provide Cloud services. Louridas provides an analysis of provider capabilities in his 2010 IEEE article. (Louridas 2010) Table 5 provides an insight into the high-level attributes of SaaS and PaaS leading public providers at that time.

Table 5 -Key features of Cloud provider offerings (Louridas 2010)

Feature	Amazon Web Services	Google App Engine	Microsoft Azure	Force.com
Service Delivery Model	IaaS	PaaS	PaaS	SaaS
Storage	Simple Storage Service (S3), Amazon Elastic Block Storage (EBS), Amazon SimpleDB, Amazon Relational Database Service (RDS)	App Engine datastore (not relational, built on Bigtable); objects with properties are stored without a schema, supporting transactions	Persistent data stored in non-relational blobs, tables, and queues; SQL storage offered by SQL Azure	Persistent data stored in objects; object instances are analogous to relational database table
Security	SAS 70 Type II Certification, firewall, X.509 certificate, SSL-protected API, access control list	SAS 70 Type II Certification, secure access to intranet via Google's Secure Data Connector	SAS 70 Type II Certification, applications run on 64-bit MS-Windows Server 2008	SAS 70 Type II Certification, access control on data based on user identity and organizational roles

Although Cloud service providers are extremely sophisticated, having adopted and integrated some of the newest IT capabilities to fuel their Cloud services, most of these Cloud providers are simply unaware of the Federal Cloud customer's complexity. (DISA 2011) As Federal agencies are growing in their understanding of Cloud, so must public Cloud service providers.

A full assessment of current Cloud providers' capabilities is beyond the scope of this dissertation. Furthermore, such an assessment, even if it was feasible for this dissertation, would rapidly become irrelevant because of the rapid evolution occurring in this relatively new area of IT. This short review, however, provides insights into the enduring characteristics and attributes of Cloud providers in general, which will be useful in refining the definitions and measures of Cloud decision factors.

Section Seven – Federal Agencies and Federal Guidance Affecting Cloud

Guidance, in terms of laws, regulations, and policy affect how both commercial and governmental enterprises acquire and manage IT capabilities. This section describes Federal Agencies and highlights the guidance that pertains to decisions on Cloud migration and is organized by themes found across multiple sources of guidance.

Federal Agencies as IT Enterprises

The US Federal Government is the world's largest consumer of information technology, with over 12,930 IT systems costing approximately $80B a year for development, modernization, and sustainment. (OMB 2009). Based on OMB, Cloud offers the potential for $20B in savings each year (see Figure 13) (Kundra 2011).

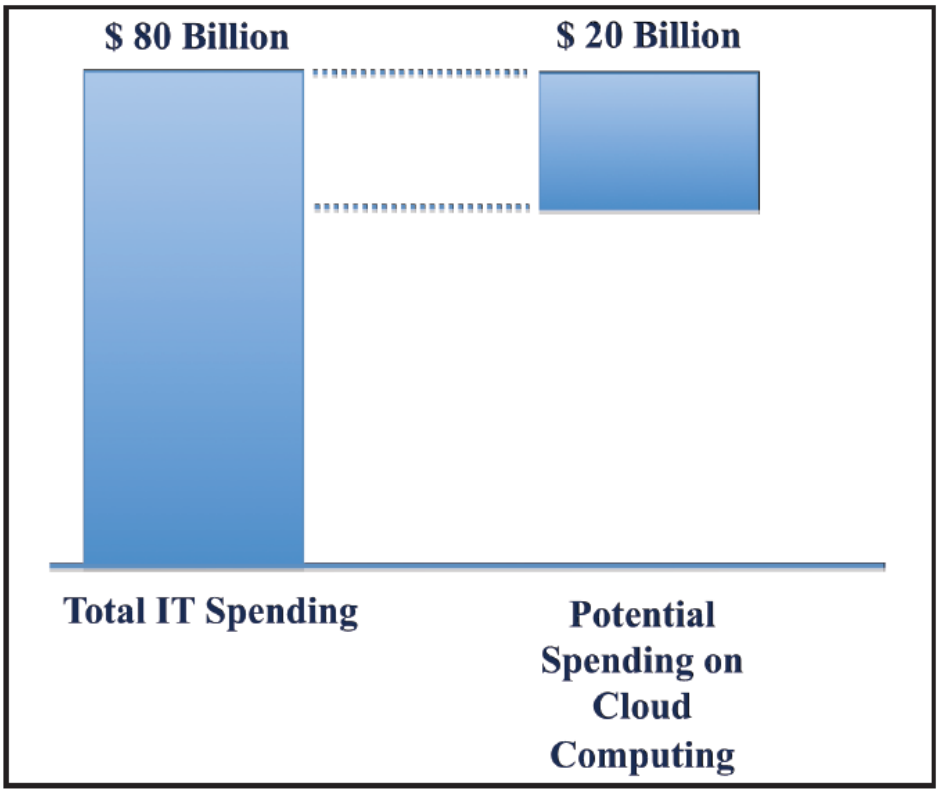


Figure 13 - Estimated portion of Federal IT spend able to move to the Cloud in 2011 (Kundra 2011)

One justification for estimating 25% savings is the ability of Cloud to share resources and balance load over more users. Industry has leveraged this Cloud concept to drive savings. Figure 13 below depicts the status of the Federal Government compared to other entities in terms a single metric – server utilization.

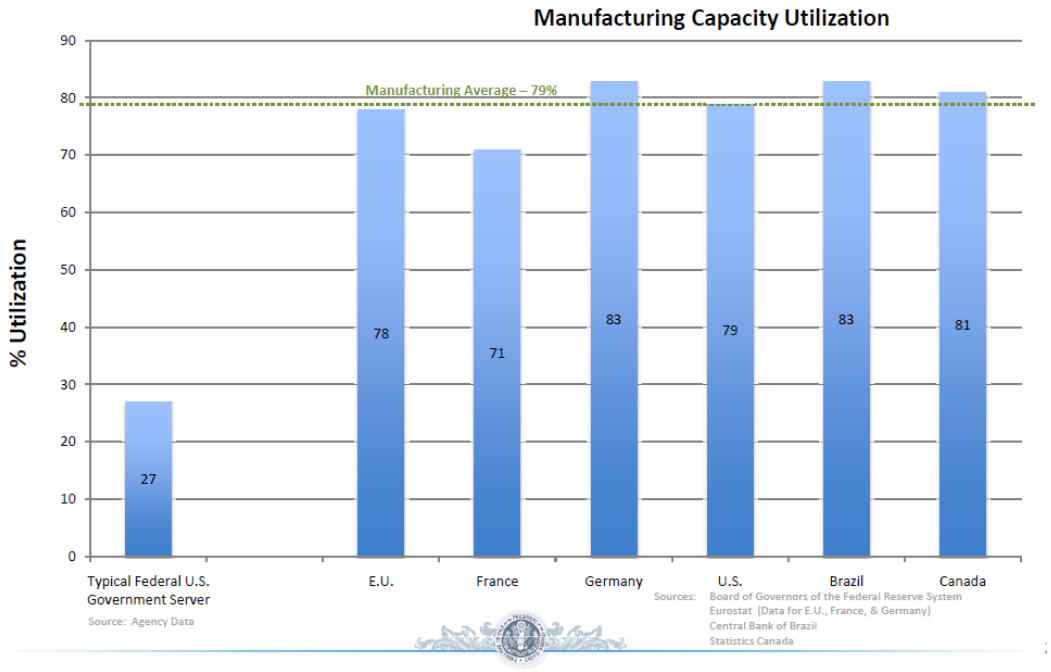


Figure 14 - Comparing Server Utilization (Kundra 2011)

The Senior IT leader within the Federal Government is the CIO. This position was created in 2002 but alternate titles were employed until Vivek Kundra served as Federal CIO. (Government 2002) Each Federal agency also has an agency CIO with specific responsibilities and authorities given to the position through Public Law 104-106 in what's now referred to as the Clinger-Cohen Act. (Congress 2006) Portfolio management, enterprise architecture, and now Cloud adoption fall under the purview of the agency's CIO.

Guidance related to failing IT projects

The Federal Government does not have a strong record for successful IT projects. Federal guidance now requires agencies to either turnaround or terminate at least one-third of underperforming projects within their portfolio over 18 months (Kundra 2010).

Federal agencies are also prohibited from funding major IT programs that lack the following: (Kundra 2010)

- A dedicated program manager and fully staffed integrated program team
- A modular approach delivering usable functionality every six months
- Specialized IT acquisition professionals

Cloud elasticity can potentially allow a project to start up quicker and avoid most up-front capital costs, lessening the chance of early failure. Also, should an IT project leveraging Cloud fail, it terminate cleaner without having to repurpose significant IT assets.

Guidance related to IT consolidation

The number of datacenters in the Federal Government has grown significantly – from 432 in 1988 to 1,100 in 2009 to 2,094 in 2010. (Kundra 2010), while commercial firms have reduced their numbers. Federal Guidance places pressure on Federal agencies to physically consolidate IT assets and reduce the number of data centers under an initiative named the Federal Data Center Consolidation Initiative (FDCCI). Guidance resulting from FDCCI includes:

- Inventory and track all datacenters (Kundra 2010-2)
- Reduce the number of datacenters by at least 800 by 2015 (Kundra 2010)
- Create a government-wide marketplace for data center availability (Kundra 2010)

This guidance is disruptive in that it requires the physical move of legacy systems. This will in turn trigger discussions and later decisions within each agency's IT governance

about the disposition of legacy systems. Such might not have occurred without the FDCCI guidance, but now these discussions open the opportunity for these agencies to consider migrating to Cloud as a potentially better option than just physically collocating IT assets. And, even for co-location of physical IT assets, by treating the datacenters as FaaS, agencies would benefit from a consistent decision framework and decision factors that span FaaS as well as IaaS, PaaS, and SaaS.

Guidance directly involving Cloud

To accelerate adoption of Cloud among Federal agencies, the Federal Government – primarily the Federal CIO – have issued progressively stronger forms of guidance. This guidance on Cloud includes:

- Shift to a "Cloud First" Policy (Kundra 2010)

  "When evaluating options for new IT deployments, OMB will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective Cloud option exists." (p 7)
- Agencies will be responsible for evaluating their sourcing strategies to fully consider Cloud computing solutions (Kundra 2011)
- Jump-start the migration to Cloud technologies (Kundra 2010)

  "Each Agency CIO will be required to identify three 'must move' services and create a project plan for migrating each of them to Cloud solutions and retiring the associated legacy systems."

In addition to this guidance to all Federal agencies about Cloud adoption, OMB directed GSA to stand up contracts for Cloud services. OMB also directed efforts to establish

templates for Service Level Agreements relating to those SaaS services that most agencies are considering, such as Cloud-based email. (Kundra 2010)

Guidance Related to Federal Procurements

To promote fair competition, ensure considerations for socioeconomics, and provide the best value for procurements, the US Government established the Federal Acquisition Regulations (FARs). Federal Agencies can extend and further elaborate on (but not contradict) the FARs through their own agency regulations, such as DoD established with the Defense Federal Acquisition Regulation System (DFARS) (AT&L 2003). These regulations affect Cloud migration decisions by prescribing both the process, and the structure of the steps leading to the final procurement.

Much has been written about how the FARs are structured as "one size fits all," lumping IT procurements together with large weapon system procurements such as fighter aircraft, ships, and tanks. Also, the FARs were originally established to support system acquisitions. Yet Cloud represents a paradigm change – Federal Agencies shift from system acquisition to services acquisition by migrating from IT systems to Cloud.

A common decision framework for migrating legacy IT systems to Cloud will not likely address these larger issues. However, a common decision framework could help agencies defend the validity of their acquisition strategy leading to the procurement. For example, the US Congress directed the US Army to temporarily halt its email migration to a DoD Community Cloud Model until the Army reported about the decision process and business case that led to the migration itself. (Army February 2012)

One requirement of very large acquisitions, that's also generally expected of less significant acquisitions such as Cloud migration, is that the acquisition decision question include an analysis of alternatives.(USD(AT&L) 2008) The nuance of this is that a common Cloud migration decision framework would benefit from including a decision question framed such that the decision is not "yes/no" – a binary decision – but rather the selection of the best alternative among multiple alternatives. Often, one of the alternatives is the status quo, which if that alternative is selected, it is equivalent to a "no" decision.

Section Eight – The US Federal Cloud Decision Framework (USFDCF)

In 2011, the Federal CIO, through OMB, published the "Federal Cloud Computing Strategy." (OMB 2011) This strategy included a framework for Cloud migration that spanned the three lifecycle phases of a Cloud migration, to include 1) selecting the systems to migrate, 2) provisioning the new capability within Cloud services, and then 3) managing the new capability within the Cloud environment. (see Figure 15)

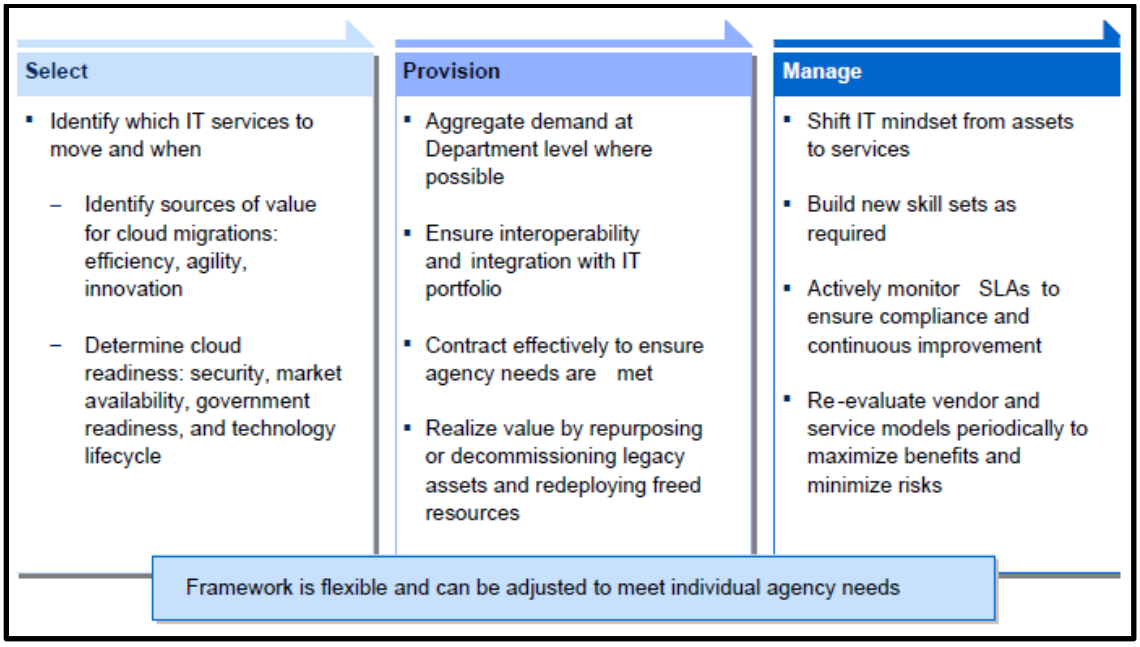


Figure 15 - Kundra Lifecycle Framework for Cloud Migration (Kundra 2011).

This research project set out to validate the first phase, of that larger Cloud migration framework – the "Select" phase. For this first phase, Kundra outlines a decision framework for selecting IT systems to migrate. This decision framework is referred to in this paper as the US Federal Cloud Decision Framework (USFCDF). As laid out by Kundra, The USFCDF can be seen as a combination of three constructs:

- The decision structure (DS), a model that relates the overarching aspects of the decision and is used to group or categorize elements of the decision
- The decision factors (DFs), the specific elements of necessary to address for the Cloud migration decision, and
- The decision question (DQ), which is how the migration question itself is formulated.

These three constructs of the USFCDF are described graphically in Figure 16.

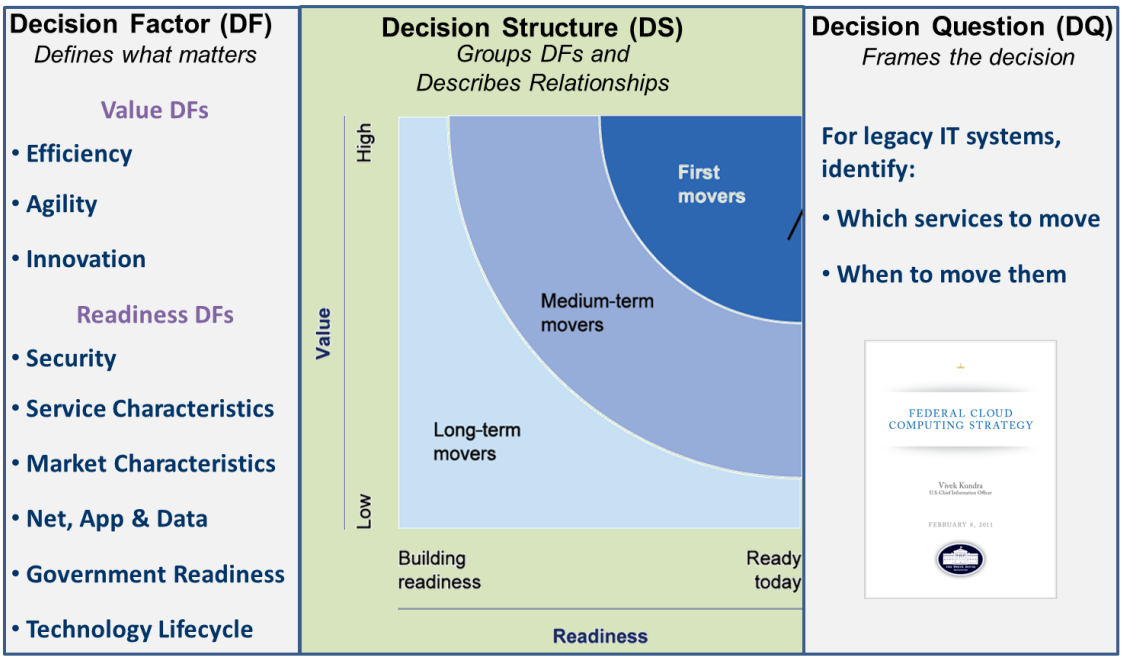


Figure 16 - Three Constructs of the US Federal Cloud Decision Framework (USFCDF)

Because this research project is centered on the USFCDF, these three constructs (DF, DS, and DQ) are provided further amplification in the following three sections.

Section Nine – USFCDF Cloud Decision Factors (DFs)

This section summarizes insights from literature and preliminary interviews related to the decision factors relevant to Cloud migration decisions. This section leads with the nine USFCDF DFs and concludes with insights on decision factors from other sources. For example, surveys, which includes surveys performed by associations and by another graduate student researcher, provide insights into the decision factors related to an informed decision on Cloud migration.

.

The remainder of this section reviews literature related to the ten decision factors of the USFCDF, starting with the decision factors related to the "Value" category of the USFCDF decision structure, then moving to the decision factors relating to the "Readiness" category of the USFCDF.

Efficiency DF

Efficiency gains can come in many forms, including higher computer resource utilization due to the employment of contemporary virtualization technologies, and tools that extend the reach of the system administrator, lowering labor costs. Efficiency improvements can often have a direct impact on ongoing bottom line costs. Further, the nature of some costs will change from being capital investment in hardware and infrastructure (CapEx) to a pay-as-you go (OpEx) model with the Cloud, depending on the Cloud deployment model being used. Services that have relatively high per-user costs, have low utilization rates, are expensive to maintain and upgrade, or are fragmented should receive a relatively high priority for consideration. Federal Cloud Computing Strategy (Kundra 2011)

Kundra also identified the value of Cloud efficiency compared to today's legacy systems. (see Figure 18)

EFFICIENCY	
Cloud Benefits	**Current Environment**
• Improved asset utilization (server utilization > 60-70%) • Aggregated demand and accelerated system consolidation (e.g., Federal Data Center Consolidation Initiative) • Improved productivity in application development, application management, network, and end-user	• Low asset utilization (server utilization < 30% typical) • Fragmented demand and duplicative systems • Difficult-to-manage systems

Figure 17 - Efficiency DF – Benefits of Cloud Compared to Current Environment

The efficiency DF describes elements of a cloud decision related to funding and costs. IT cost savings remain important to IT leaders in large organizations. IT leaders consistently rank cost savings as one of their highest priorities – as noted in Figure 20 later in this chapter.

Cloud potentially enables efficiency not only by the better utilization of processing power, but also by the labor savings inherent in moving to Cloud. William Forrest, an analyst at McKinsey credited with several Cloud studies indicated that a move to Cloud would save 15% of labor costs associated with the legacy IT system. (Forrest 2009) Mark Forman, former E-Gov Chief for the Office of Management and Budget, stated publically that Cloud could save 90% to 99% of the operating cost of an IT system. (CSIS 2009) Ted Alford and Gwen Morton, in their study of Cloud, predicts savings of 50-67%. (West 2010) Rajen Sheth, moderator of the Google Enterprise Blog, states that from his analysis with Google, a migration to Cloud email will save 67%.

Others though, are not so sanguine. Forrest believes that, when the transitional costs of the actual migration are included in the analysis, Cloud may cost 44% *more* than legacy hosting. (Forrest 2009)

Why the wide variations in estimated savings? One reason these analyses vary widely is that they are primarily predictions because Federal agencies have had little experience in using Cloud long enough to generate data on the savings. Another reason for the variances in efficiency is that different delivery and deployment models will affect the financial analysis. For example, a private Cloud is likely to be less efficient than a public Cloud. The reason can be found in an earlier section of this Chapter -- on page 21 under resource pooling. Resource pooling, and its complement, multi-tenancy, drive savings through better utilization of resources and economies of scale. But, a private Cloud deployment model by definition limits the users to those in the Cloud's owning organization. A private Cloud implies no multi-tenancy and reduced resource pooling. Alfred and Morton in 2009 analyzed Storage as a Service, a subset of IaaS, and concluded that 1,000 file servers would cost $22.5M from a public Cloud provider but nearly 50% more ($31.1M) for the same capability on a private Cloud. (Morton 2009)

A final challenge in realistically measuring efficiency is that, by definition, this factor is the difference between the cost of the new Cloud service and the cost of maintain the legacy system. Because a Cloud service provider's business model depends on knowing costs, Cloud service providers generally publish prices, providing a ready source of the "to be" costs. Yet the true total costs of a legacy system may be difficult to assess, making the calculation of efficiency – the delta between the "to be" and the "as is" –

difficult as well. In the Federal government, the problems calculating efficiency is further compounded because the organization migrating to Cloud might not be paying the total costs of ownership for the legacy system. For example, facilities, security, licensing, electricity, and other aspects of the total cost of ownership may be borne by organizations other than the IT organization within the Agency. However, the organization migrating the legacy system will likely be responsible for paying all costs associated with the migration itself and the subsequent Cloud services.

Agility DF

Many Cloud computing efforts support rapid automated provisioning of computing and storage resources. In this way, Cloud computing approaches put IT agility in the hands of users, and this can be a qualitative benefit. Existing services that require long lead times to upgrade or increase / decrease capacity should receive a relatively high priority for consideration, and so should new or urgently needed services to compress delivery timelines as much as possible. Services that are easy to upgrade, are not sensitive to demand fluctuations, or are unlikely to need upgrades in the long-term can receive a relatively low priority.

Federal Cloud Computing Strategy (Kundra 2011)

Kundra also identified the value of Cloud agility compared to today's legacy systems. (see Figure 18)

AGILITY	
Cloud Benefits	**Current Environment**
• Purchase "as-a-service" from trusted cloud providers • Near-instantaneous increases and reductions in capacity • More responsive to urgent agency needs	• Years required to build data centers for new services • Months required to increase capacity of existing services

Figure 18 – Agility DF – Benefits of Cloud Compared to Current Environment

Although not concisely defined in the Federal Cloud Strategy (see above), Kundra describes agility in terms similar to NIST's definition of rapid elasticity – value from Cloud's ability to scale up and down responsively.

Research supports the value of agility as a decision factor. According to a 2011 survey of Federal IT leaders, most think their IT capital planning process is too slow and clumsy to react quickly to changes in capital funding. (TechAmerica 2011). These same IT leaders felt the capital planning process needs to shift its focus from infrastructure to meeting business and mission requirements. Cloud's agility provides value to a Federal IT leader because a Cloud service provider can quickly adjust services to respond to changing needs and funding changes.

Cloud not only can provide Agility in terms of budgeting, it also provides agility for rapid development as well as response to rapid, and perhaps unanticipated, surges in user demand. Vivek Kundra, provided this example at his Congressional Testimony before a special joint session on Cloud:

I want to point you to the next slide, which is a tale of two cities. In the first story, how the Government deployed an IT system versus how a private sector company deployed an IT system. When we deployed a Cash for Clunkers program, we deployed the traditional

approach to IT, and as demand grew, the system was unstable and continued to crash over a 30-day period, and we had to literally reengineer the solution, buy new hardware and configure it.

Yet, a company called Animoto faced similar problem but was using Cloud technology. With 250,000 new users enrolled over a 3-day period, they were able to scale from 50 virtual machines to over 4,000 virtual machines and supported, at peak times, 20,000 new users an hour. (Kundra 2010-2)

As a final benefit, IaaS provides a standard infrastructure platform, allowing Federal IT Leaders to focus on the applications and data central to their business and mission requirements. By applying a systems engineering approach toward separation of concerns, Cloud enables Federal organizations to focus on their unique needs, and not be slowed by also having to engineer portions of their system not core to their unique needs.

Innovation DF

Agencies can compare their current services to contemporary marketplace offerings, or look at their customer satisfaction scores, overall usage trends, and functionality to identify the need for potential improvements through innovation. Services that would most benefit from innovation should receive a relatively high priority

Federal Cloud Computing Strategy (Kundra 2011)

Kundra also identified the value of Cloud innovation compared to today's legacy systems. (see Figure 19)

INNOVATION	
Cloud Benefits	**Current Environment**
• Shift focus from asset ownership to service management • Tap into private sector innovation • Encourages entrepreneurial culture • Better linked to emerging technologies (e.g., devices)	• Burdened by asset management • De-coupled from private sector innovation engines • Risk-adverse culture

Figure 19 – Benefits of Innovation to Current Environment

Kundra's description of innovation is admittedly a bit imprecise, but based on the benefits listed from innovation, this decision factor represents capabilities achieved by migrating to Cloud beyond what was possible from the legacy system. The innovation is not the Cloud capability itself, but rather what the organization can do – and perhaps do faster – for its customers by tapping the Cloud and the innovation building on Cloud capabilities. Kundra lists the following benefits of Innovation: (Kundra 2011)

- Shifts focus from asset ownership to service management
- Taps into private sector innovation
- Encourages entrepreneurial culture
- Links better to emerging technologies (e.g. devices)

Kundra contrasted the benefits above with the barriers of today's IT environment listed below:

- Burdened by asset management
- De-coupled from private sector innovation engines
- Risk-adverse culture

Security & Privacy DF

Federal Government IT programs have a wide range of security requirements. Federal Information Security Management Act (FISMA) requirements include but are not limited to: compliance with Federal Information Processing Standards agency specific policies; Authorization to Operate requirements, and vulnerability and security event monitoring, logging, and reporting. It is essential that the decision to apply a specific Cloud computing model to support mission

capability considers these requirements. Agencies have the responsibility to ensure that a safe, secure Cloud solution is available to provide a prospective IT service, and should carefully consider agency security needs across a number of dimensions…

Federal Cloud Computing Strategy (Kundra 2011)

For a Federal IT leader making decisions about Cloud migration, security would also include concerns for protecting privacy information. Furthermore, the requirements for security go beyond actually securing the data – a plethora of Federal guidelines require compliance through specific actions and reporting. Furthermore, some of these actions and reporting may not be practical in a Cloud environment.

The Federal Cloud strategy lists the following security considerations: (Kundra 2011)

- 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, and provide the

information necessary for the agency to appropriately and independently assess and monitor the efficacy of those controls.

The 2011 survey of Federal IT leaders by TechAmerica found that their paramount concern is cyber security. (TechAmerica 2011) This same group is hopeful that FedRAMP, a government initiative related to security discussed earlier (Chapter 2, Section Seven – Federal Agencies and Federal Guidance Affecting Cloud) will help address the Cloud security challenges.

Within the Federal government, DoD is often the agency most concerned with security. It stands to reason that the most sensitive information related to our national interests and national security would reside within DoD. DISA is the IT provider for DoD. At the request of the Program Executive Officer for DISA, the Armed Forces Communications and Electronics Association (AFCEA) hosted a one-day technical exchange with leaders of DISA, industry, academia, associations, and other Federal agencies. The AFCEA planning committee devoted six months to prepare for this technical exchange, drawing upon the AFCEA Technology Committee, DISA security leaders, and external expertise such as the President of the Cloud Security Alliance. Collectively, the committee determined the highest priority questions for DISA related to Cloud. DISA's three top security questions fell into three categories: (Mink 2010)

- Cloud security policy and guidance
    - How does security policy and guidance need to change/evolve for the Cloud infrastructure?

    - How does security policy and guidance need to change/evolve for deploying applications and services to the cloud?
    - How does responsibility and accountability change in the cloud?
- Cloud security architecture and technology
    - What are the software and data concerns for the Cloud architecture?
    - What are the hardware security concerns in the cloud?
    - How do we lay a secure foundation for transparency in the Cloud environment?
- Secure Cloud operations
    - How do we establish a baseline for a secure Cloud environment?
    - How do we monitor, identify, and respond to problems in the cloud?
    - How do we maintain assured command and control in the Cloud environment?

Cloud providers already are familiar with standardized and verified security standards. For example, the approach for FedRAMP to provide centralized security and privacy certification incorporates an approach adopted by Cloud providers to verify compliance with security standards for commercial users -- Statement on Auditing Standards No. 70: Service Organizations (SAS 70) Type II certification. (Louridas 2010)

Service Characteristics DF

Service characteristics can include service interoperability, availability, performance, performance measurement approaches, reliability, scalability, portability, vendor reliability, and architectural compatibility.

Storing information in the Cloud will require a technical mechanism to achieve compliance with records management laws, policies and regulations promulgated by both the National Archives and Records Administration (NARA) and the General Services Administration (GSA). The Cloud solution has to support relevant record safeguards and retrieval functions, even in the context of a provider termination.

Depending on the organizational missions supported by the Cloud capability, Continuity of Operations (COOP) can be a driving solution requirement. The purpose of a COOP capability is to ensure that mission-essential functions continue to be available in times of crisis or against a spectrum of threats. Threats can include a wide range of potential emergencies, including localized acts of nature, accidents, and technological and/or attack-related emergencies.

The organization should consider scalability requirements concerning the ability of the Cloud solution architecture to either grow or shrink over time, with varying levels of processing, storage, or service handling capability. They should also consider both the impact on their business processes if network connectivity to their Cloud provider fails, resulting in a loss of IT capability, and the possibility (likelihood) of this occurrence.

Requirements concerning administrative support should be included as well, covering topics such as the daily hours of prime support, problem escalation times, resolution of recurring problems, and trouble ticket submission methods.

Federal Cloud Computing Strategy (Kundra 2011)

The capabilities, both technical and managerial, of a Cloud service provider affect a Federal agency's decision to migrate to Cloud. Kundra suggests an initial set of service characteristics that would shape the data collection effort for this decision factor. These characteristics are: service interoperability, availability, performance, performance measurement approaches, reliability, scalability, portability, vendor reliability, and architectural compatibility. (Kundra 2011)

One characteristic absent from Kundra's list is "familiarity with customer environment." Many commercial organizations have embraced Cloud. However, familiarity with commercial customers may not always translate into understanding of Federal customers. Commercial Cloud providers can drive down costs by leveraging multi-tenancy to create economies of scale. Yet, these commercial providers usually do not appreciate the complexity of doing business with a Federal customer. (Orndorff 2010) Federal contractors, on the other hand, work closely with Federal agencies through multiple contracts. These Federal contractors are very familiar with the complexity of Federal IT acquisitions. However, Federal contractors usually lack in-place infrastructure to provide Cloud services. Furthermore, the Federal customers' concern for security has limited multi-tenancy and therefore some of the cost efficiencies. But, an even more significant barrier for Federal contractors to provide Cloud services is the manner in which Federal funds are budgeted. In particular, Congress often provides funding one year at a time. Therefore Federal agencies can usually only commit to one year's Cloud funding at a time. Cloud services require significant capital investment up front, and without a multi-year commitment from Federal customers, a single year does not provide a cost-effective

business model. Federal contractors remain reluctant to assume the risk of large outlays up front with no guarantee of future year revenue. Multi-year IT budgets can provide Federal IT leaders with flexibility that would therefore enable more Federal contractors to become Cloud providers. (TechAmerica 2011)

Market Characteristics DF

Agencies should consider the Cloud market competitive landscape and maturity, including both fully commercial and government-provided Cloud services. Agencies can consider whether Cloud markets are sufficiently competitive and are not dominated by a small number of players. Agencies can consider whether there is a demonstrated capability to move services from one provider to another, and whether there is a demonstrated capability to distribute services between two or more providers in response to service quality and capacity. Agencies should consider the availability of technical standards for Cloud interfaces which reduce the risk of vendor lock-in.

Federal Cloud Computing Strategy (Kundra 2011)

While the service characteristics described above apply to each specific Cloud service provider, this decision factor – market characteristics – applies to the Cloud service provider marketplace overall. According to the Federal Cloud Strategy, "Agencies can consider whether Cloud markets are sufficiently competitive and are not dominated by a small number of players. Agencies can consider whether there is a demonstrated capability to move services from one provider to another…" (Kundra 2011)

DoD shares this concern about vendor lock-in also. During opening remarks at the 2010 Technical Exchange on Cloud Security, DISA emphasized the importance of avoiding vendor lock-in when considering Cloud. (DISA 2011) DISA noted that the forms of vendor lock-in included user interfaces and data migration. Six months later, as DISA prepared to recompete Defense Connect Online (DCO), DoD's SaaS Cloud offering for collaboration, DISA realized that users had stored data in virtual "meeting rooms" unique to the vendor providing DCO. After consulting industry, DISA found it would be impractical to migrate the data to a competing DCO Cloud provider. Because the data was locked into the current vendors DCO Cloud service, DISA was locked into the current DCO contractor. As a result, DISA was forced to offer the incumbent contractor a sole-source contract extension for up to four additional years. (DISA 2011)

Network Infrastructure, Application, and Data Readiness DF

Before migrating to the Cloud agencies must ensure that the network infrastructure can support the demand for higher bandwidth and that there is sufficient redundancy for mission critical applications. Agencies should update their continuity of operations plans to reflect the increased importance of a high-bandwidth connection to the Internet or service provider. Another key factor to assess when determining readiness for migration to the Cloud is the suitability of the existing legacy application and data to either migrate to the Cloud (i.e., rehost an application in a Cloud environment) or be replaced by a Cloud service (i.e., retire the legacy system and replace with commercial SaaS equivalent). If the

candidate application has clearly articulated and understood interfaces and business rules, and has limited and simple coupling with other systems and databases, it is a good candidate along this dimension. If the application has years of accumulated and poorly documented business rules embedded in code, and a proliferation of subtle or poorly understood interdependencies with other systems, the risks of "breakage" when the legacy application is migrated or retired make this a less attractive choice for early Cloud adoption.

Federal Cloud Computing Strategy (Kundra 2011)

Kundra groups this decision factor along with the next decision factor (below) in his Federal Cloud Strategy as one combined factor, "Network infrastructure, application, and data readiness." By breaking the original decision factor into two parts in this research, this first half, Network & Infrastructure, better aligns with one of the five Cloud characteristics, which is broad network access. Also, by changing "network infrastructure" to "network & infrastructure," this decision factor encompasses enterprise infrastructure other than just network infrastructure to inform decision makers for successful Cloud deployments. For example, as in February 2010, DISA and the US Army CIO were both optimistic they could roll out SaaS -- enterprise email -- to 1.4 million users by September 30, 2011. Yet, about one month prior to that target date, enterprise email only reached 8,900 users. (Hale 2011) According to John Hale, the DISA program manager for enterprise email, the primary reason for the delay was that the Army network was not architected for an enterprise. (i.e. Network) Even more insightful though was Hale's mention that nonstandard desktop computer configurations

were even a larger problem than the Army's network in rolling out enterprise email (i.e. general infrastructure). (Hale 2011)

Application and data readiness indicate whether the application can be migrated to Cloud using IaaS or PaaS, or that the necessary data from the application can be migrated to SaaS. For example, a legacy system running on an older version of the Solaris operating system might not find a Cloud service provider willing to host the application because of too little demand to merit the capital expense to support a little-used OS. Similarly, legacy Federal financial systems may not be able to export their data in a format compatible for ingestion into a SaaS offering for financial services.

Application and Data readiness also demonstrates that some decision factors interact with others. Application and Data readiness affects the efficiency decision factor. For example, as DISA developed its Enterprise Email (EE) Cloud service, DISA repurposed the Microsoft Exchange licenses held by the US Army, DISA's first EE customer. Thus, the legacy applications not only were not only ready to migrate to SaaS, but they also freed up licenses that could then be used by the enterprise email Cloud services provider(Hale 2011). Of course, some Cloud providers cannot leverage such licenses or the software vendors might prohibit such use in their license agreement(Plant 2011).

Government Readiness DF

Agencies should consider whether or not the applicable organization is pragmatically ready to migrate their service to the Cloud. Government services which have capable and reliable managers, the ability to negotiate appropriate

SLAs, related technical experience, and supportive change management cultures should receive a relatively high priority. Government services which do not possess these characteristics but are otherwise strong Cloud candidates should take steps to alleviate any identified concerns as a matter of priority.

Federal Cloud Computing Strategy (Kundra 2011)

Government readiness indicates whether the Federal agency has the skill set to manage IT capabilities as services as well as whether the organization itself is pragmatically (culturally) ready to operate using Cloud services. (Kundra 2011) The first consideration – the skill set for managing IT capabilities as services – includes expertise on defining, evaluating, and managing Service Level Agreements (SLAs). Talent within the organization will also need to be able to assess the capabilities of Cloud service providers.

Cultural readiness remains a pragmatic consideration as well. Today, many Federal agencies lack familiarity and understanding of Cloud. Highlights of a survey by Market Connections Inc. found that: (IMJ 2010)

- Thirty-four percent of respondents are not familiar with the Cloud
- Twenty-one percent of professionals involved in cyber security at their agencies are unaware of Cloud computing
- Only fourteen percent said their agencies have adopted Cloud computing
- Twenty-three percent don't know what their agencies are doing with Cloud computing

The same survey also indicated that the greater knowledge of Cloud, the more professionals trust the Cloud and do not consider it a leading security vulnerability. This supports the notion that an objective framework with decision factors related to Cloud migration would not only lead to better decisions about Cloud migration, but that the framework and objective decision process will itself contribute to increasing a Federal agency's knowledge of Cloud and therefore its readiness to adopt Cloud.

Even commercial firms – credited with adopting Cloud more readily than Federal agencies, have limited familiarity with Cloud. Forrester Research Inc. surveyed large companies to determine their intentions for adopting Cloud. Forrester reported the following: (Plant 2011)

- Interested, but no plans (39%)
- Not interested (37%)
- Planning to implement in the next 12 months (7%)
- Expanding/upgrading implementation (5%)
- Implemented, not expanding (1%)
- Don't know (2%)

Forrester's research indicates that only 6% of large companies had already adopted Cloud.

Another cultural aspect that affects organizational readiness is the perception of control. As one Federal CIO noted, "Internal squabbling may hinder success, and the biggest barrier is a culture that thinks you have to own something to control it." (TechAmerica 2011) The term sometimes heard regarding cultural immaturity is "box hugging." Yet,

the concern with control and ownership might not be just emotional – existing organizational incentives may hinder the acceptability of transferring ownership to a Cloud provider. For example, government employees associated with legacy systems may feel their jobs are at risk should a system migrate to Cloud. Similarly, Federal contractors may see their revenue dry up as the systems they sustain move to a Cloud provider. Together, the issue of control and ownership remains a concern for organizational readiness to migrate legacy applications to Cloud.

Federal agencies considering Cloud face a constraint usually not shared with commercial firms, which is Federal Acquisition Regulations (FAR) and other Federal guidance affecting IT decisions. One example of such a constraint is guidance to set aside contracts exclusively for small business. As noted by the Program Executive Officer for Mission Assurance, Mark Orndorff, DISA is constrained by acquisition rules such as small business goals. (Orndorff 2010)

Technology Lifecycle DF

Agencies should also consider where technology services (and the underlying computing assets) are in their lifecycle. Services that are nearing a technology refresh, approaching the conclusion of their negotiated contract, or are dependent upon inefficient legacy software or hardware should receive a relatively high priority. Technology services that were recently upgraded, locked within contract, and are based on leading-edge technology may want to wait before migrating to the Cloud.

Federal Cloud Computing Strategy (Kundra 2011)

The previous five DFs focused on whether Cloud providers and the government agency were ready (and able) to migrate a legacy system to the Cloud. This final USFCDF DF is more related to the timing of the migration. Kundra indicates that timing may depend on the state of the legacy technology or the constraints of current contracts. Technology that's no longer commercially supported or technology that cannot be maintained might indicate urgency for a migration. On the other hand, current robust hardware and software may have significant slack capability to serve an organization for quite some time without requiring additional resources or significant sustainment challenges – suggesting the migration could be delayed. This discussion about the timing for refreshing or transforming the technology stack applies not only to the more obvious capital purchases of hardware and software, but also to capabilities procured through licenses. In particular, software licenses often have durations, suggesting that some points in time are best suited for their termination or transfer.

The temporal aspect of the technology lifecycle applies not only to the technology stack itself – both capital purchases and licensing -- but also to the wetware, which is the personnel sustaining the technology stack. In the Federal Government, agencies often procure personnel support from contractors. These contracts have lifecycles as well, which often influence the timing of transformations such as a migration to Cloud.

Additional Insights on Cloud Decision Factors

A survey by the nonprofit Public Technology Institute (PTI) found wider adoption of Cloud by local governments. 45% of local governments are using some form of Cloud

computing. (IMJ 2010) This same survey identified the following factors local governments felt important for adopting Cloud:

- Resource Savings (87%)
- Features (48%)
- Availability and uptime (45%)

Applying these three factors to the USFCDF, the first two of these factors would be appear to fall under USFCDF "Value" category – factors which determine the benefit of migrating to Cloud. The latter factor (availability and uptime) appear reflective of the USFCDF "Readiness" category – factors that help decide whether the Cloud provider is ready to replace the legacy IT system.

In another survey of Federal agencies, 70% of those surveyed are most concerned about security, including privacy and data integrity. (IMJ 2010) Clearly, these two factors fall within the USFCDF "Readiness" category as they moderate the final migration decision by indicating whether the Cloud providers and the Federal Agency are ready for a successful migration.

The Wall Street Journal, in an article on Cloud for business, noted two basic decision factors: "Is this move [to Cloud] going to save money, and will it bring better technical results?" (Plant 2011) These two appear to be "Value" considerations.

In yet another survey, TechAmerica surveyed forty-six IT Federal IT Leaders in 2011. Their top three budget priorities were: "lowering costs; integrating systems and processes; and implementing security and privacy measures." See Figure 20.

Priority	Ranking
Lowering costs	1
Integrating systems and processes	1
Implementing security and privacy measures	1
Project management improvements	4
Staff development/retention/ recruiting	5
Transparency and performance management initiatives	5
Stimulus support	7

Figure 20 - TechAmerica Survey of 46 Federal IT Leaders (TechAmerica 2011)

Based on the researcher's professional experience, there may be factors specific to the US Federal Government that may affect Cloud migration decisions. For some Federal Agencies such as DoD, funds are often "fenced," which means the funds are restricted to certain types of expenses or investments. For example, DoD receives separate appropriations for "Other Procurement – appropriation 3080" and for "Operations and Maintenance – appropriation 3400." Traditional IT procurement falls under the first appropriation, and costs such as utility expenses fall under the latter. Congress restricts how funds for one appropriation might be applied for another appropriation. Traditionally, Federal agencies acquired new IT capabilities or directed development of

these new IT capabilities. But Cloud can be considered utility computing. Much like electricity and water utilities, Cloud computing becomes an operating expense for a Federal enterprise, and would fall under a different appropriation than purchasing IT systems outright. Depending on the Federal organization, this "color of money" may make a Cloud migration more or less feasible. Federal IT leaders need definition on "what constitutes operations and maintenance (O&M) versus development?" (TechAmerica 2011) Appropriations and other forms of a funding restriction is a likely decision factor for Cloud migration decisions. This insight was uncovered through literature research and interviews subsequent to Kundra publishing his Value/Readiness framework and associated decision factors, but may need to be considered by Federal IT leaders as they decide whether a legacy IT system should be migrated to Cloud.

Another potential DF related to the US Federal Government is compliance. Organizations may be accountable for complying with evolving rules and regulations. "As part of a comprehensive effort to increase the operational efficiency of federal technology assets, federal agencies are shifting how they deploy IT services. OMB issued a "Cloud First" policy in December 2010 that requires federal agencies to implement cloud-based solutions whenever a secure, reliable, and cost-effective Cloud option exists; and to migrate three technology services to a Cloud solution by June 2012." (Kundra 2010) US Federal IT leaders – those likely to make Cloud migration decisions – will likely consider such guidance an additional decision factor in their Cloud migration decisions.

Section Ten –USFCDF Decision Structure (DS)

The USFCDF includes a decision structure for migrating legacy systems to Cloud. This structure places the decision in the context of two dimensions: value and readiness. The value dimension captures the benefits gained by a Federal agency migrating a legacy system to Cloud. The readiness dimension broadly captures the ability for the legacy system to move to the Cloud in the near-term. Systems with relatively high value and readiness are strong candidates to move to the Cloud first. (Kundra 2011)

These two dimensions, as well as their combined impact on a Cloud migration decision, are depicted in Figure 21.

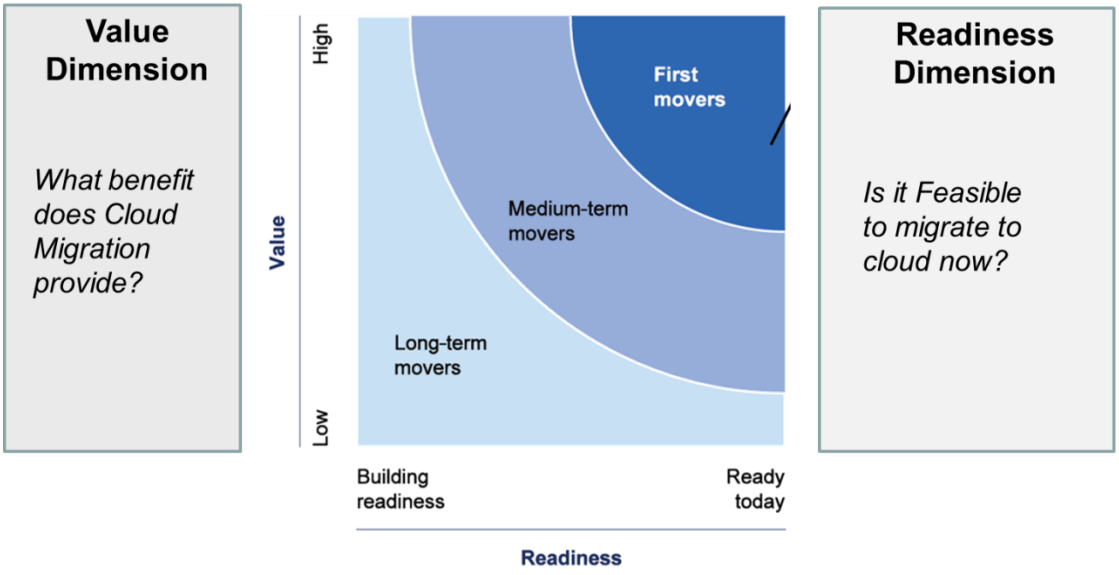


Figure 21 – The Two-dimensional structure of the Kundra Decision Framework (Mink 2011) based on (Kundra 2011)

The two dimensions (value and readiness) each contain decision factors that relate to that dimension. This section will continue the discussion of the overarching decision

structure. Discussion of the individual decision factors which comprise each of the dimensions is deferred to the next section of this paper. .

The USFCDF decision framework is consistent with prior work on selecting and evaluating IT. In 1985 Dr. Edgar Sibley published an article in The Journal of Information Systems Management about how to select and evaluate a database management system. (Sibley 1985) The issues he discussed relate strongly to this research project. For example, Sibley framed the outcome in terms of leasing or buying the DBMS software package – a rough parallel between owning a legacy IT system and paying for usage from a Cloud service provider. Sibley also suggested sources of information on his decision factors as well as approaches for depicting the data collected into a decision package.

Researchers have produced a significant body of knowledge on the topics of technology adaption and decision models for technology employment. This research explores the factors affecting acceptance of new technology and as well as the factors for selection of the best technology choice among competing options.

One model often applied to measure technology acceptance was conceived by Fred Davis in the 1980's and aptly named the Technology Acceptance Model (TAM). See Figure 22

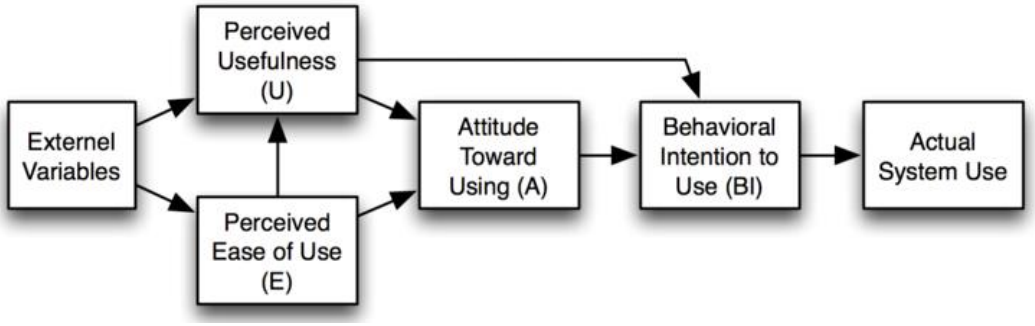


Figure 22 - Technology Acceptance Model (Davis 1989)

Davis, by leveraging prior work, concluded there were two determinants especially important for determining what causes people to accept or reject information technology: perceived usefulness and perceived ease of use. Deeper examination of the definitions and sources for Davis's two determinants strongly supports a claim that Davis' two determinants map very well onto the two dimensions of Kundra's decision structure. For example, Davis further defines perceived ease of use in terms of "freedom from difficulty or great effort," which closely relates to readiness. Davis also discusses how a cost-benefit framework differs from his usefulness-ease paradigm. The usefulness-ease framework better accommodates subjective factors in the decision. This is particularly applicable to Cloud migration decisions as some of the decision factors, particularly those in the readiness dimension, may be hard to quantify beyond subjective assessments. For example, government readiness includes not only an assessment of Cloud-related skills, but also an assessment of the organizations cultural predisposition to change.

Davis also prefaces each of his two determinants with the modifier "perceived." This is in line with conclusions of Dr. Schum about the incorporation of information into Bayes' rule and the formation of "inference networks" to show the relationship between evidence, and the evidence about the evidence. (Schum 2009) Although Kundra's two dimensions lack a similar preface or qualifier, it's unclear whether this was an oversight or an intentional approach because of how such a qualifier might be viewed within the Federal Government.

Davis's original TAM provides some validation of Kundra's value-readiness dimensions. Paul Pavlou evaluated acceptance decisions related to e-commerce in 2003 by applying the theory of reasoned action (TRA) to TAM. (Pavlou 2003) Pavlou observed that trust and risk were factors in decisions relating to adoption of e-commerce. and that by incorporating them into TAM, they improved his e-commerce acceptance model. Surveys on Cloud acceptance by senior IT leaders in the Federal Government indicate that risk, particularly security risk, is a leading factor in their decision to adopt Cloud. Furthermore, government readiness, a decision factor suggested by Kundra and described in the next section, indicates that cultural readiness, including trust, remain important factors in the Cloud migration decision.

More recently Tara Behrend and her colleagues researched Cloud computing adoption and usage at community colleges. (Tara Behrend 2011) Behrend found the two determinants of TAM to be applicable for Cloud adoption at community colleges. They also identified a strong correlation between familiarity of Cloud and adoption of Cloud. Although community colleges are not managed within the Federal Government, they are

public organizations providing community services. Furthermore, her study supports Kundra's use of readiness as his second dimension. Growing familiarity of Cloud by a Federal agency is, by itself, likely to affect an agency's decision regarding future Cloud adoption.

MITRE supports research in Cloud and has earned credibility, including a recommendation as one of the handful of resources listed in the US Government's Cloud Strategy. (Kundra 2011) In 2010, two MITRE researchers, Geoffrey Raines and Lawrence Pizette, published their findings in a MITRE Technical Paper on Federal Cloud decisions. (Pizette 2010) They focused primarily on the process steps for Cloud decisions. Their decision process depicts three steps leading to the Cloud decision: service definition, business case, and Cloud service requirements. They also depict a high-level binary decision outcome: Cloud Use or No Cloud Use. Raines and Pizette's preparatory steps provide insights for gathering data on decision factors. They also expand their "Cloud Use" binary decision outcome into three sub-decisions: public Cloud, community Cloud, and private Cloud. In other words, a decision to adopt Cloud implies an explicit decision to adopt one of the Cloud deployment models. Although this research project does not attempt to apply the Kundra decision framework to granular decision outcomes spanning Cloud deployment models, Raines and Pizette's discussion does indicate that data collected on the decision factors may need to be packaged with an eye toward the best suited deployment model. Without framing the decision in terms of a deployment model, the decision maker may not feel adequately informed to make the Cloud migration decision.

Section Eleven – USFCDF Decision Question (DQ)

The DQ is the third construct of USFCDF described in Kundra's Select Phase of the Cloud lifecycle framework published in the Federal Cloud Computing Strategy of 2011. The Select Phase can be better appreciated in the context of the other two phases Kundra outlines in his larger lifecycle framework. (see Figure 23)

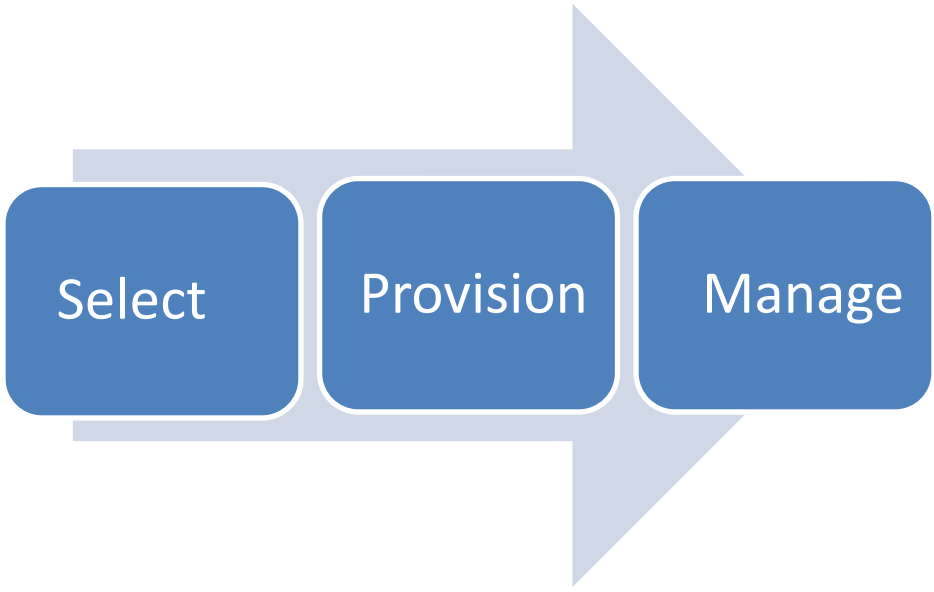


Figure 23 - Three Phases of Kundra's Lifecycle Framework. The First Phase incorporates the USFCDF DQ.

In the first phase, the Cloud Strategy directs Federal Agencies to "Identify which IT service move and when?" (Kundra 2011) This drives each Federal Agency to review their portfolio of IT services and ask themselves "Which IT systems should I migrate to Cloud and when?" Bringing this down to the level of a specific IT system, the USFCDF DQ becomes "*Should the legacy IT system migrate to cloud soon?*"

At the system decision level, the DQ drops the temporal question of "when" (other than assuming "soon") because, given the workload and resource limitations of a Federal IT Agency, it will not be practical for an IT organization to spend a lot of effort to formally make a detailed decision now for an action that will not be executed in the reasonable future. A lot can happen between now and then – in terms not only of technology, but also of policy, regulations and stakeholder preferences.

Section Twelve – Trends and Initiatives Likely to Affect Cloud Adoption

This section describes trends and initiatives that may affect how decision factors influence decisions tomorrow. For example, the Federal Government is instituting a standard security architecture and monitoring protocol for Cloud (FedRAMP). This may affect an agency's evaluation of Cloud migration readiness by eliminating some of the concerns regarding security.

Trends in Cloud Technology

The technologies underpinning Cloud continue to evolve. Taken together, these technology advancements will increase the value of Cloud and lessen the readiness gap for migrating legacy systems to Cloud. Some examples of emerging Cloud technologies include:

- Holomorphic data encryption (Gentry 2011)
    - Allows computations to be performed on encrypted data
- Digital fingerprinting (Oprea 2011)
    - Provides verification that data stored in the Cloud hasn't been maliciously altered or accidentally corrupted

- HAIL (Cloud RAID) (Oprea 2011)
    - Lets users divide data among multiple Cloud providers in such a way that if one provider goes offline, the missing information can be reconstructed from the data stored by the others.

Trends in Organizational Readiness

Several surveys and researchers have noted that as an organization gets familiar with Cloud, perhaps through lower risk migrations to Cloud, that they are more willing to move other systems to Cloud. (TechAmerica 2011)

Security is a primary area of concern for Federal agencies. Yet, these agencies are realizing that their own in-house IT is becoming increasingly vulnerable and protecting it has become increasingly expensive. Also, as noted earlier, Cloud technology for security enhancements continues to evolve. The trend is that the perceived gap between in-house security and Cloud security should shrink and perhaps reverse. This trend is already occurring for the commercial sector. When IDC asked businesses in 2008 what factors were most likely to discourage their use of Cloud computing, 72% of small businesses (defined as having fewer than 100 employees) and 63% of mid-sized companies (100 to 999 employees) said security was their chief worry. Yet, only three years later, their concern for the security gap dropped to 50% and 47% respectively. (Bussey 2011) These same firms also doubled their Cloud adoption over this same timeframe.

Similar to their private counterparts, Federal IT leaders see security consuming considerable IT resources – and that trend continues to grow. "Security cost drivers are the 24/7 nature of some operations and the associated expense of the highly skilled

people we need. Plus, it [SIC] very hard to implement these tools across a department with many component organizations and systems." (TechAmerica 2011) As this trend towards more security – and more expensive security – grows in the Federal space for legacy systems, planned initiatives such as FedRAMP and continued progress in Cloud security technology indicate that Federal IT leaders will follow commercial counterparts and see Cloud security as less an obstacle, and more a benefit.

Another trend in Federal agencies is a shift in focus from building IT infrastructure to meeting business and mission requirements. (TechAmerica 2011) This trend indicates increased value of IaaS and PaaS for Federal agencies.

"Efficiency" will also continue its importance to Federal IT leaders. In particular, CIOS will focus on gaining operations and maintenance savings (O&M consumes 70% of some CIO budgets). (TechAmerica 2011)

Cloud changes the nature of the discussion for IT. Instead of discussing systems, Federal agencies discuss services. Instead of systems interfaces, Federal agencies discuss Service Level Agreements (SLA's). Instead of integrating hardware to host an application, IT professionals provision new computing capabilities. Together, this indicates a change in the nature of the Federal agency talent required to manage Cloud which when in place, should mature an organizations readiness to adopt Cloud. Some Federal CIOS have noted this, indicating in a recent survey their desire to "shift the talent base from developing systems to smart buying." (TechAmerica 2011)

Trends in Standards & Policy

As the importance of Cloud grows, universities, Federal agencies, and nonprofits are sprouting or expanding to address Cloud issues. Once example is the Cloud Security Alliance, a global organization who early-on recognized that security was a major issue with the growing Cloud movement. (Alliance 2009) After a meeting between the researcher and the President of CSA in 2010, CSA agreed to support the November 2010 DoD technical exchange on Cloud Security. At this conference they introduce the concept of the security cube. (See Figure 24) Following that event, CSA established its second US chapter and located it in the Washington DC area in part to address Federal Cloud security issues. CSA is but one example of a growing body of organizations, talent, and knowledge focused on Cloud. As this body of knowledge grows and addresses Cloud issues, Federal organizations should see a trend of increasing value and increasing readiness to migrate legacy applications to Cloud.

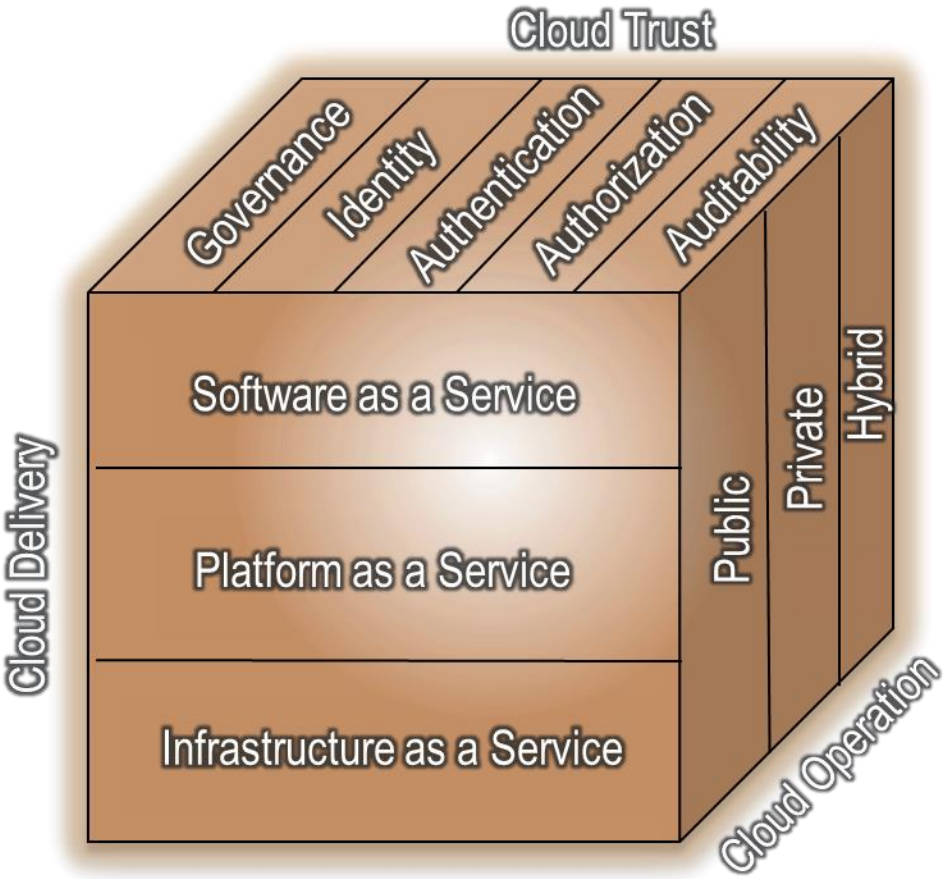


Figure 24 - Cloud Security Alliance Mission: Develop a trusted reference architecture to leverage the Cloud delivery models in a secure manner regardless of the delivery model

Perhaps the most significant initiative affecting Cloud migration in the future is the Federal Risk Assessment and Management Program (FedRAMP). FedRAMP is an inter-agency initiative to provide a unified, government-wide risk management process for Cloud computing. (Council 2010) The Federal Government established a common set of security standard levels, and then uses third parties to assess a Cloud service providers against those standards. Cloud service providers benefit by architecting and operating their Cloud services to a common security standard. Agencies gain from FedRAMP

because they can reference the third party security assessment and avoid performing a similar security assessment themselves. NIST notes that multitenancy is a characteristic of Cloud. FedRAMP avoids the requirement for each of those tenants to perform a duplicative security assessment of the same Cloud service. FedRAMP also benefits the Cloud service provider, because the Cloud service provider need only establish one security approach, and then have it validated (assessed). That validation can then be used to satisfy multiple customers. Figure 25 depicts how FedRAMP changes security from a many-to-many arrangement for security, to a one-to-many using a common security approach and assessment.

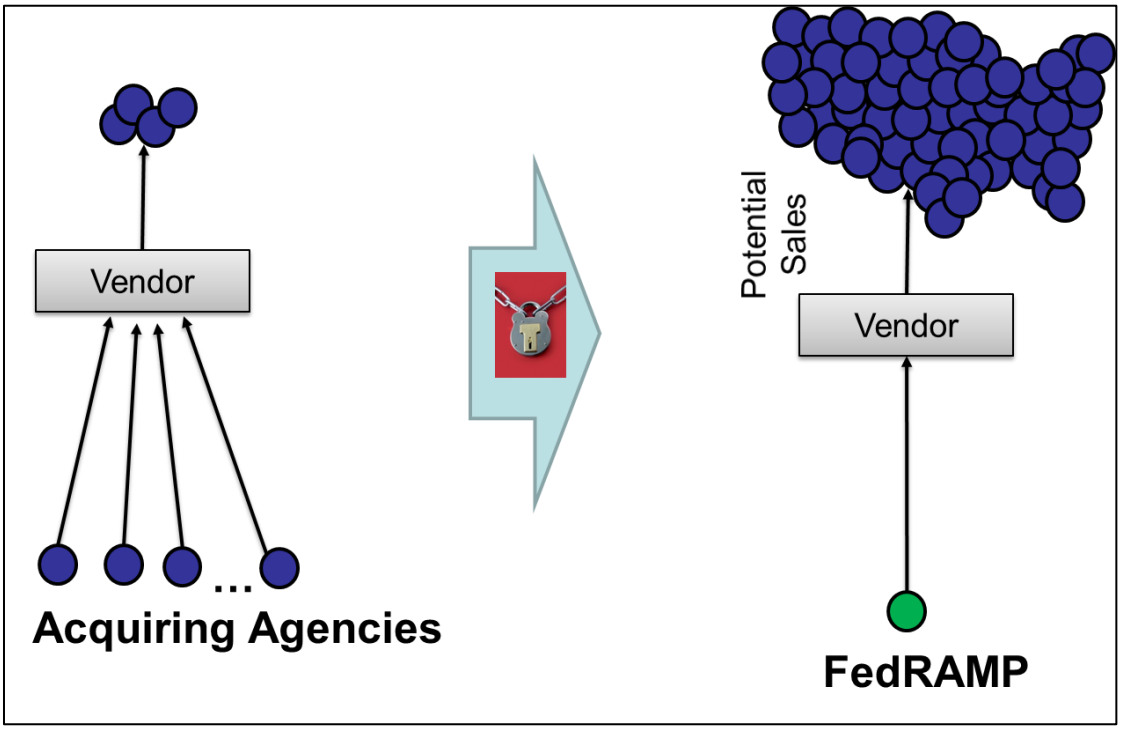


Figure 25 - FedRAMP reduces effort for security compliance. (Council 2010)

Section Thirteen – Systems and Systems of Systems

This research topic is particularly relevant to the body of knowledge for systems engineering.

Prior work indicates that organizations adopting Cloud will need expertise designing and managing services by employing service level agreements (SLAs). This move to services and SLAs follows nicely with the growing body of knowledge in systems engineering related to services engineering. Several years ago, DoD expanded the Department of Defense Architectural Framework (DoDAF) from a focus exclusively on systems to also include services.

In addition to the services-approach of Cloud that ties to services in DoDAF, the layered nature provided by NIST's three service delivery models, with the two additional layers suggested previously in this paper, suggests a fit with the enterprise approaches advocated by James Martin in his 2006 doctoral research on knowledge modeling and hierarchy of architectures. (Martin 2006)

The migration of systems to Cloud also represents a shift in the responsibility domain between government and contractors for information systems. (see Figure 26)

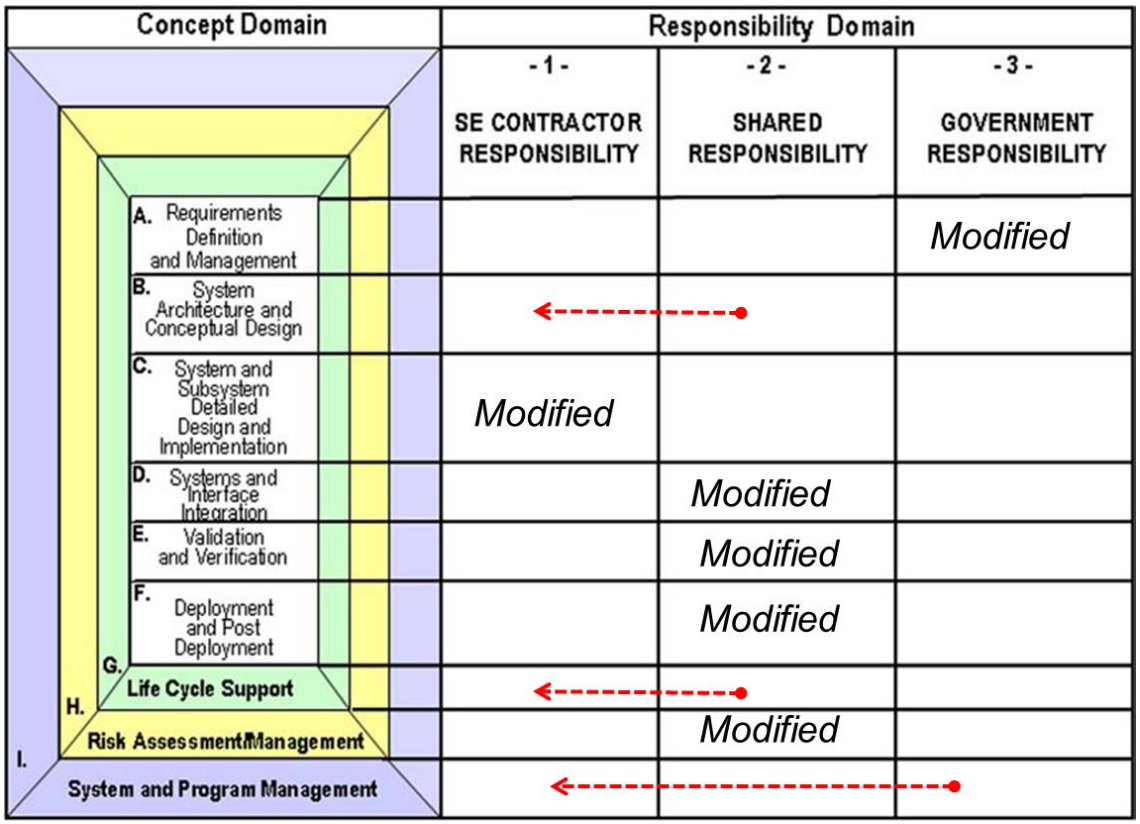


Figure 26 - A framework of key systems engineering concepts and responsibilities (Friedman and Sage 2003) - with annotations related to Cloud.

This research project should also expand the body of knowledge on Systems of Systems, as Cloud represents a form of Systems of Systems. The three rather different approaches the government may choose for acquiring capability in a SOS construct are: (Carlock 2001)

- Government awards a prime SOS engineering contract to a single systems engineering (and integration) firm
- Government acts as integrator, awarding multiple, smaller contracts for each of the component systems

- Government awards a contract for an integrator, but government also awards the contracts for the component systems

Cloud adoption represents a potential use of any one of those three acquisition approaches, driven by the Cloud hosting environment and the legacy system migrating to that environment.

Overall, this research project touches on several topics of interest today in systems engineering, and although not the specific focus of this research project, the research work may expand the body of knowledge for these topics.

3. RESEARCH METHODOLOGY

This research project investigates the decision framework and decision factors associated with a US Federal Government agency decision to migrate an existing (legacy) information technology (IT) system to the Cloud. Aside from a few surveys – to include one survey-based master's dissertation – little research has been accomplished in this specific area.

This chapter surveys potential research methodologies and then outlines the rationale for selecting the multicase study (aka multiple-case study) methodology for this research project. Having adopted the multicase methodology, this chapter then details the specifics of this research project based on the six-step multicase study construct outlined by Robert Yin and further informed by Robert Stake. Yin's six-step construct encompasses both the research plan itself as well as topics related to the research methodology, such as research validity, research instruments, role of the researcher, investigative privacy/confidentiality, etc. Stake's contributions increase the robustness of Yin's construct, particularly as they pertain to this research project.

Analysis of Competing Research Methodologies

This section analyzes the various research approaches available to answer the research questions and concludes by arguing multicase study, the most rigorous variant of the general case study methodology. Orlikowski and Baroudi, in their study of research

approaches and assumptions for information technology in organizations, outlined the most prevalent research methodologies in Table 6 (Orlikowski 1991). Each of these research designs has potential applicability to the general area of Cloud research in the US Federal Government. Of these, several are particularly applicable to the research questions about Cloud migration decisions.

Table 6 - Articles Classified by Research Design Methodology (Orlikowski 1991)

Research Design	Frequency (Rounded to nearest %)
Survey	49%
Laboratory Experiment	27%
Case Study	14%
Mixed Method	3%
Field Experiment	3%
Instrument Development	3%
Protocol Analysis	1%
Action Research	1%

These research designs are examined each in turn.

Survey Methodology

Gartner, Forrester, and IDC have each surveyed Federal IT leaders about their concerns and in some cases, expected benefits of adopting Cloud. One researcher, an Army Captain at the Air Force Institute of Technology, took the IDC survey and focused on DoD IT leaders. (Killaly 2011) Another researcher used separate survey questions applied to commercial firms. These surveys collectively furthered the body of knowledge on Cloud adoption, primarily by identifying which issues IT leaders feel affect the feasibility of Cloud Adoption greatest. Furthermore, additional surveys would

benefit this domain by addressing gaps in knowledge, such as identifying feasibility factors missing from earlier surveys or identifying the factors IT leaders feel affect the value or benefit of Cloud adoption the most.

Existing surveys have not focused on IT leaders who had already made decisions about Cloud migration. The surveys targeted attitudes of IT leaders in general and did not differentiate whether these IT leaders had actually made decisions affecting Cloud migration. Furthermore, given the limited understanding of this relatively new technological capability, it's likely that IT leaders will have widely differing views of what constitutes Cloud. This is evident by analyzing the 78 examples 25 Federal agencies nominated for Cloud migration. Several examples appeared to consider re-architecting a client-server application to a web-based application as a Cloud migration. Therefore, while there are opportunities for surveys to further extend the body of knowledge related to Cloud adoption in Federal Agencies, a survey-design would not adequately answer the research questions in this paper.

Laboratory Experiment Methodology

The next research method, laboratory experiment, would be difficult, if not impossible to adopt for this research given that the variability in this study is the people within the experiment. Furthermore, it's unlikely that non-essential variables could be held constant and that no control case could be adopted for comparison.

This brings us to the next research method – case studies.

Case Study Methodology

.

The case study method investigates what Robert Stake, a contemporary case study researcher and author, describes as a quintain, which is "an object or phenomenon or condition to be studied."(Stake 2006) This research project focuses on such a quintain – the decision to migrate a legacy IT system to the Cloud. Early use of the case study typically focused on decision-related quintains. For example, over thirty years ago, William Schramm, in his working papers on case study research, noted that "the essence of a case study, the central tendency among all types of case study, is that it tries to illuminate a decision or set of decisions…" (Schramm 1971) This indicates that the case study may be an appropriate methodology for this research topic.

Robert Yin, perhaps the leading case study researcher today, provides an operating definition of this methodology:

A case study is an empirical inquiry that:

- *Investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident.(Yin 2009)*

Yin also provides these characteristics of the case study inquiry:

- *Copes with the situation in which there will be many more variables of interest than data points, and as one result*
- *Relies on multiple sources of evidence, with data needing to converge in a triangulating fashion, and as another result*
- *Benefits from the prior development of theoretical propositions to guide data collection and analysis.*

Yin's characterizes three situations when a case study would be applicable : (Yin 2003-2) All three of these situations are in concordance with this research project:

- ✓ *The type of research question asks "how" or "why"*
- ✓ *The case represents contemporary phenomenon in a real-life context.*
- ✓ *The researcher has little or no possibility to control the events*

One variant of the single case study is the multicase study, also referred to as the multiple case study and multiple-case studies by various researchers. Yin describes the multicase study as "a single empirical inquiry or study that contains two or more cases." (Yin 2012) Yin considers the multicase study as a stronger and potentially more desirable research method because multiple cases provide a broader array of evidence than do single cases. This greater body of evidence can be applied to either cover the same focused set of research issues more intensely or alternatively, allow more issues within a general them to be addressed.

Yin notes the downside of multicase studies, to include:

- *More effort*
- *May require a team of researchers rather than a solo investigator*
- *Often require external funds as a source of support.*

Yin concludes that "though the efforts [of a multicase study] are more costly, sponsors benefit because they have greater confidence in findings that are not based solely on a single case." (Yin 2012)

Action Research Methodology

Incorporating the researcher in the case study itself is a characteristic of a less-often used research design called action research (AR). By definition, AR is a future (not historical) case study within an informed Federal agency. The researcher would be a coach as well as an observer, acting as someone familiar with the decision framework and associated decision factors. Future-based case study design could be accommodated by application of a single case study.

One of the leading contemporary thinkers in AR is Richard Baskerville. Baskerville is a Professor at the School of Management at The Binghamton Centre of The State University of New York. Baskerville supports arguments for applying AR as a design for research such as this research project because "it is grounded in practical action aimed at solving an immediate problem while informing theory." (Baskerville 1999)

AR is change-oriented. For this research project, the introduction of the Kundra Value-Readiness framework and associated decision variable introduces change into the IT decision-making process. And because the USFCDF has not yet been applied to a Federal Cloud migration, it's impossible to investigate a case study that adopted the USFCDF.

AR is not without some disadvantages however. As noted by Peak in his research, "Action research is hard to arrange and hard to achieve. A reason for the rarity of scholarly action research in IT literature is that few companies will allow external academics the opportunity to tinker with their organization or its processes." (Peak 2011)

A significant challenge for applying an AR design for this research will be to find a Federal Agency willing to allow a researcher to participate in an activity that affects the

agency's IT decisions. A secondary challenge for action research is to account for the effect of the researcher as a participant within the research project itself.

Other Research Design Methodologies Considered

In addition to surveys, laboratory experiments, case studies, and action research, other research designs include: field experiments, instrument developments, protocol analysis, and mixed methods. These other research designs did not prove adequate to support answers to the research questions posed in this dissertation. They either required the researcher to control the situation – which is highly unlikely for a Federal Government agency – or they were not applicable for early exploratory research in an emerging area such as migration to Cloud.

Selected Methodology – Case Study (Multicase Study)

The nature of the research problem, the relatively recent introduction of Cloud computing, and the paucity of prior research on the specific topic of migrating legacy IT systems to Cloud computing in a Federal agency, together suggest research on this topic will require exploratory research methodologies. The two best research methodologies for initial exploratory research are action research and case studies.

As little as two years ago, few Federal agencies had migrated legacy systems to Cloud. At that time, the only feasible research methodology would have been action research. During the last two years, The US Federal Government made several decisions to migrate legacy systems to Cloud. Although these decisions did not apply the USFCDF, they do provide sufficient data about the decision factors for Cloud migrations to support one or more case studies. Therefore, the case study research methodology is a better choice than

the action research methodology for this research project. Furthermore, there appear to be enough Cloud migration decisions to employ the multicase study methodology, which increased the rigor and provided additional support to the findings. It also appears, through extensive literature study and inquires of IT Federal IT leaders, that no prior case study research has been accomplished on this topic to date[2].

The qualitative and quantitative research methodology applied to this research project was a multiple case study of recent decisions about Cloud migration leveraging Kundra's USFCDF.

Application of Multicase Study Methodology to this Research Project

The research methodology employed for this project is multicase study. This section outlines the research project using the six steps of the research cycle for the multiple case study (CS) research method proposed by Yin. This is portrayed graphically in Figure 27.

[2] The US Federal Government has published documents about Cloud adoption using the term "case study," but those reports fell short of research papers and did not investigate the Cloud migration decision.

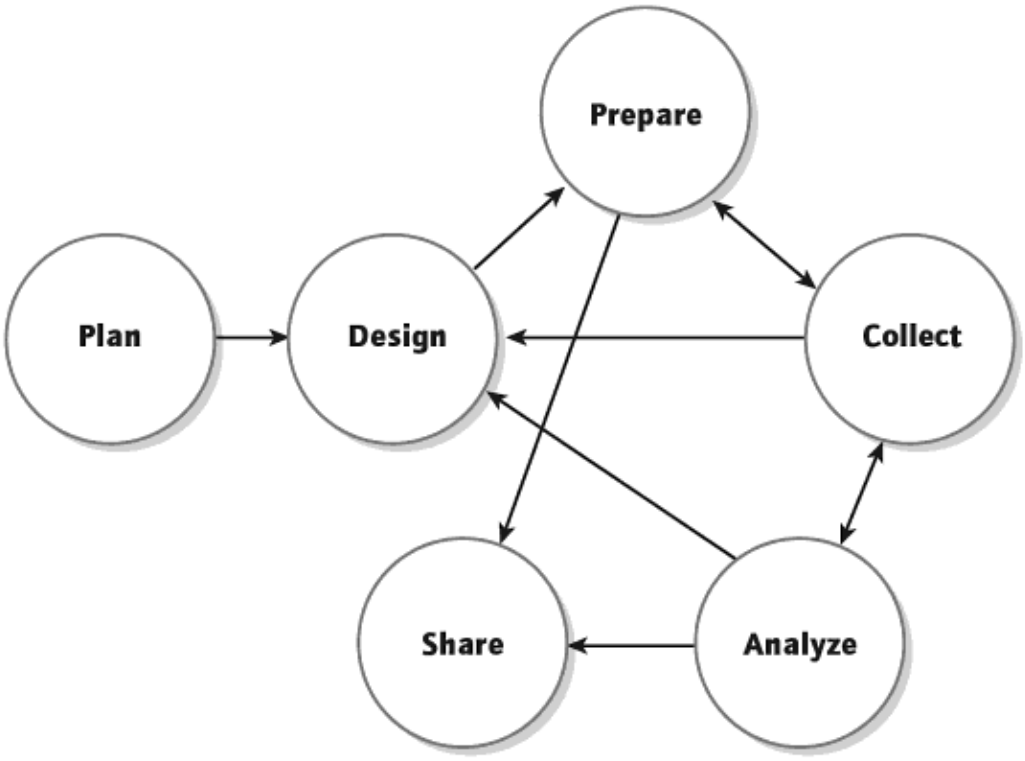


Figure 27– Case Study Cycle (Yin 2009)

Although Yin depicts the interaction of these steps, they can be rolled flat in to sequential phases. The following six sections of this chapter align with Yin's template and are depict the phases of the methodology:

Phase 1 – Planning: Identify research purpose, problem statement and research questions

Phase 2 – Designing: Identify cases and establishing the logic of the case study

Phase 3 – Preparing: Develop study protocol and obtain approvals

Phase 4 – Collecting: Gather data in accordance with research principles

Phase 5 – Analyzing: Examine evidence to draw empirically-based conclusions

Phase 6 – Sharing: Report results

CS Phase 1 – Planning

This section describes the research purpose, problem statement and related research questions. Traditionally, this phase also provides the rationale for the selected research methodology. This project will apply the multiple case study as the appropriate variant of case study research as described earlier in the section titled: Selected Methodology – Case Study (Multicase Study).

Purpose of the study

The purpose of the study is to further knowledge of, and potentially provide a solution to the problem regarding a Federal agency's ability to decide whether a particular IT system should be migrated to Cloud.

Through research actions, the study will also provide greater clarification on the meaning and measures of the decision factors as they relate to the Cloud IT decision. This should transform Kundra's model from a concept to a validated, usable framework.

Finally, by adopting a CIO-prescribed model and evaluating it in a Federal agency following academic research standards, the resulting framework should convey credibility and validity for wider adoption across all Federal agencies.

This purpose closely fits with the Pattern Matching, one of two techniques Friedman and Sage cite for using a case study. See Table 7.

Table 7 - Two closest case study techniques for analyzing case studies (Friedman and Sage 2003)

Pattern Matching	Explanation Building
Pattern matching contrasts and compares an empirically observed pattern with one that is predicted. This might be used, for example, to compare our case study to one found in the literature. Here a researcher develops a prediction about patterns expected to be seen in collected data. The associated analysis attempts to determine the pattern that best corresponds to observed data. The major difficulty with this approach, assuming, of course, that it is possible to collect the relevant data, is to decide upon how close is the "fit" of the data to a predicted pattern. Much researcher interpretation and judgment may be needed	Here, the researcher analyses data by building up an assumed explanation about the case. The purpose of this is to analyze the case study data by establishing an explanation about the case. This is usually accomplished by linking events and issues causally. This approach goes beyond pattern matching in that specification of the nature of the links, usually causal, between elements that make up the pattern is a hoped for result. The researcher then tests the evidence for the relationships.

Problem Statement

The Federal government is the largest acquirer and maintainer of IT systems globally. (Kundra 2010-2) Federal agencies spend over $80M to maintain nearly 13,000 IT systems. (OMB 2009) Furthermore, the US Government's citizens, and in some cases citizens of the global community often depend on the US Government for security and services, which in turn are reliant on this large portfolio of IT systems. Throughout the history of this nation, new technologies have increased the US Government's ability to provide security and services. Cloud technologies have the potential to divert $20B of unnecessary spending to other higher value purposes while simultaneously providing Federal agencies additional advantages in terms of agility and innovation. (Kundra 2011)

Today, Cloud is a relatively new technology. While Cloud can provide advantages to both new and existing legacy IT systems, 70% of Federal IT resources are spent on supporting legacy systems. Furthermore, increasing budget constraints suggest limitations on future "green field" IT systems. Congruent with the Pareto Principal, Cloud will have the greatest impact on legacy "brown field" systems within the US Government. Yet in the past, technology adoption was often slowed, or poor technology choices made, until responsible Federal agencies developed trust in their ability to make decisions about the new technologies.

The problem is that *"Federal Agencies lack a common, validated decision structure for deciding whether a legacy IT system should migrate to the Cloud."*

Research Scope

Cloud is a very broad research area. This research projected was constrained so that the overall effort would remain feasible while the results would retain impact and significance. The scope of the research project was consciously delimited (bounded) in the following ways:

Cloud Delivery Model (constrained to Software as a Service): NIST identified three delivery models for Cloud (IaaS, PaaS, and SaaS). Further investigation suggested two other delivery models (FaaS and AaaS). (See Chapter 2, Section 2) This scope of this research is constrained to just one of those five delivery models; SaaS, although it could be argued that the research conclusions could be generalized to all delivery models.

Cloud Deployment Model (constrained to exclude Hybrid Cloud): NIST identified four deployment models for Cloud (Public, Private, Hybrid, and Community). This research

omitted hybrid Cloud and is constrained to include only Public, Private, and Community Cloud.

Target Organizations (US Federal Agencies): the problem described in the previous subsection clearly applies globally and to all organizations considering Cloud capabilities. This research is constrained to investigate only government organizations, in the US, and at the Federal level. Specifically, this excludes non-US organizations, commercial/business firms, and lower level governmental organizations such as state and local governments.

Target IT System (legacy email): Cloud can provide many SaaS capabilities. This research is does not investigate the decision framework for new capabilities from Cloud, but rather is constrained to explore the migration of a legacy system to Cloud. This is significant in that a recent GAO report concluded that such migration comprised nearly two thirds of the new Cloud capabilities in the Federal Agencies they studied (the other third were new capabilities). (Government Accountability Office 2012) The research is further constrained to investigate only back-office systems, specifically email, a form of office automation and collaboration. Although email is fairly specific, it can arguably be generalized to other well-defined enterprise IT systems.

The figure below summarizes the scope of the research, serving as a simplified systems context diagram from a systems engineering perspective.

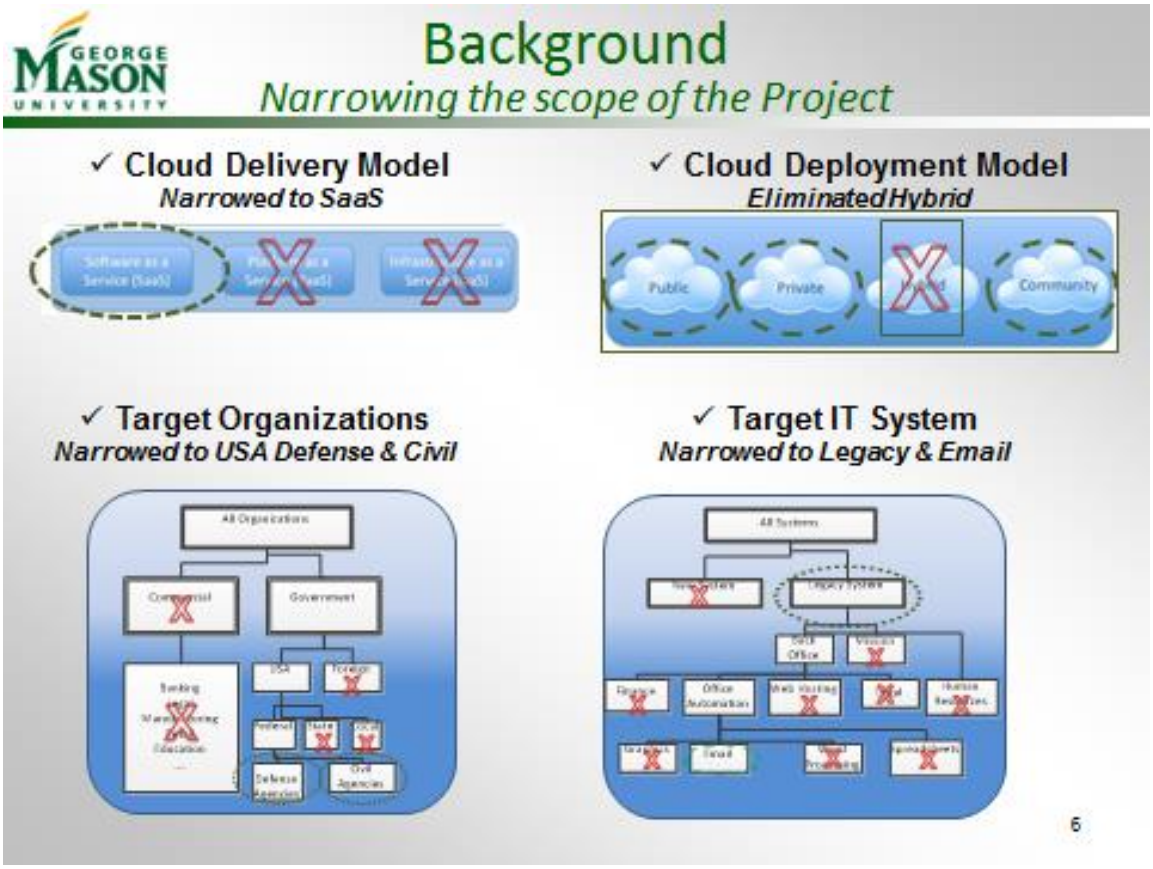


Figure 28 - Constraints on Scope of the Research Project

Research Questions

This study will attempt to answer three primary questions and associated subquestions as shown in Table 8.

Table 8 - Research Questions and Subquestions

Questions & Sub-questions
1. Do the USFCDF **decision factors** provide value to Federal IT leaders deciding whether a legacy IT systems should migrate to the Cloud?
a. Are all USFCDF decision factors necessary?
b. Is the set of USFCDF decision factors sufficient?
2. Does the USFCDF **decision structure** provide value to Federal IT leaders deciding whether a legacy IT systems should migrate to the Cloud?
a. Does a decision structure (in general) provide value?
b. Is the Value-Readiness paradigm of the USFCDF decision structure useful for marshalling decision factors?
3. Does the USFCDF **decision question** provide value to Federal IT leaders deciding whether a legacy IT systems should migrate to the Cloud?
a. Is the USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions?
b. Is the USFCDF decision question consistent with the needs of the decision maker?
4. Is email a well-defined legacy IT system?
a. Are email systems in the Federal defined by a small set of similar legacy commercial products?
b. Is email used across the Federal enterprise?
5. Would Cloud migration decision-makers have benefited from prior-knowledge of a validated USFCDF?

Question 1 is a primary research question around the factors considered for the decision to migrate to Cloud. These factors were identified using the same resources and codified in the same documents as USFCDF discussed in the previous subsection. The specific decision factors for this research are described in Chapter II and synthesized later in this

chapter. Using the list of factors recommended by the former Federal CIO as a baseline, this question is answered by decomposing the question into three related subquestions. Subquestion 1a determines whether all the USFCDF decision factors are necessary. This question implies investigation into the prioritization (importance) of each USFCDF decision factor relative to the other USFCDF decision factors. This is similar to sensitivity analysis in that knowledge of which decision factors are primary and which are secondary can allow future decision makers to prioritize their pre-decisional activities and also prioritize the influence of factors on their actual decision. Because this research answers this question for particular systems – in a particular contexts – the nature of the systems and the contexts may preclude the results of 1b from being generalized to other systems or other contexts.

Subquestion 1b attempts to compare the decision factors actually employed by decision makers to those posited by the Federal CIO to ascertain whether the set of USFCDF decision factors were sufficient. Preliminary study by the researcher indicates that Kundra's decision factors will prove useful in making Cloud migration decisions, but that at least one factor may be absent – specifically a factor that would consider the constraints imposed by external guidance on IT decisions. An example of this is Congressional guidance restricting Federal Agencies on how IT funds can be spent for activities that include Cloud-based IT. The comparison to Kundra's set of DFs is to actual decisions is important to either validate Kundra's recommendations or suggest refinements to his set.

Question 2 relates to the overall decision structure suggested by Kundra that groups the decision into two categories, each with its own corresponding set of decision factors. The Kundra framework parallels the two categories of factors Davis's widely accepted Technology Acceptance Model (TAM). See Figure 29 - Technology Acceptance Model (Davis 1989)

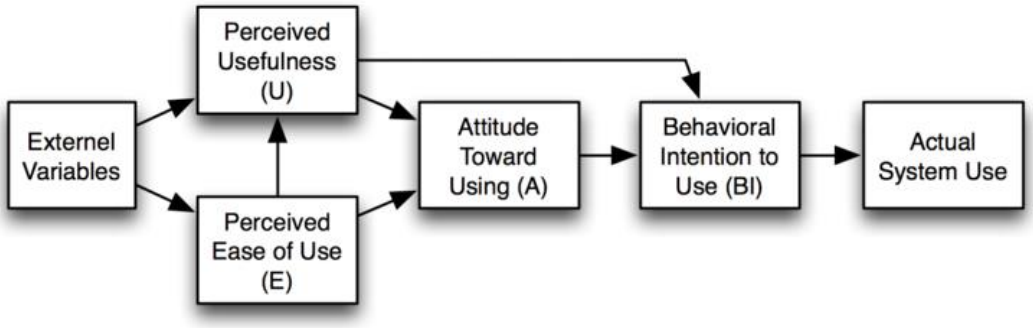


Figure 29 - Technology Acceptance Model (Davis 1989)

Davis notes that "people tend to use or not use an application to the extent they believe it will help them perform their job better" and then refers to this as "perceived usefulness (U)." (Davis 1989) For Cloud, the parallel is that organizations, in particular the IT decision makers in Federal agency, will tend to use Cloud to the extent they feel it will help their organization perform its function better. In the case of Kundra's framework, "better" includes more efficiently, which in turn is often consider as cheaper.

Davis also defines a second determinate of technology acceptance – perceived ease of use (E). "Ease of Use" is defined by Davis as "the degree to which a person believes that using a particular system would be free of effort," in other words, freedom from difficulty or great effort. Kundra's "Readiness" determinant indicates how hard – or easy – it would be for the Federal agency to move the legacy system to Cloud. By casting this set of decision factors as readiness instead of ease of use, Kundra implies that the ease of implementation changes over time and that, like preparing for an event, the organization can improve the factors that drive readiness for legacy migration.

This research project will only analyze activity through the step described by Davis as "Behavioral Intention to Use" (BI), which is defined for this research project as the time when the Federal agency makes their decision on a target system using the Kundra framework. Importantly, this research does not attempt to determine the efficacy of the decision. Research on the subsequent migration efforts and the value of the migration to Cloud is beyond the scope of this research. One benefit of focusing the research on the Cloud decision – and not the subsequent result of the decision – is that the data for the earlier phases is more likely to be accessible and less likely to be biased by those in the organization who may be motivated to depict a successful outcome from the decision.

Question 3 advances the research beyond determining necessary decision factors and associated decision structure by asking whether it is feasible for an organization to apply the USFCDF decision question compliant with the legal and regulatory requirements for a soliciting a commercial contract in support of a Federal Agency. If the Federal agency cannot legally use the USFCDF to prepare and justify a contract for commercial services

such as Cloud, then the USFCDF is unlikely to be adopted, at least not in the near future. Furthermore, if the decision question cannot be portrayed in a form that's actionable for the decision on the best approach for acquisition, then the USFCDF is also likely to be unusable.

Question 4 is necessary to support a generalization in the scope of the research results. This project researches one type of legacy IT system – email. The researcher anticipates that the research will determine that email is well-defined because it's similar across Federal Agencies and has been adopted across the Federal enterprise. Therefore, the finding for email would generalize to other well-defined legacy systems, such as standard storage systems, phone systems, word processing systems, spreadsheet systems, etc.

Question 5 is not related to the hypothesis itself, but rather to the significance of the research. Based on preliminary exploratory interviews, the researcher anticipates that decision makers would value a validated USFCDF because it would improve and accelerate their decision about Cloud migration, while also providing a defensible rationale for how they framed the migration decision.

Anticipated Findings and Resultant Hypothesis

Prior work, to include recent surveys of commercial and federal IT leaders, informed this research project and provided insights into anticipated findings. The researcher anticipated that the USFCDF, with a slight evolution, can provide value to Federal IT decision makers in determining whether a well-defined legacy IT system should migrate to the Cloud. In particular, the researcher anticipated that a Federal IT leader would find each of the three elements of the USFCDF of value to include:

- The decision factors
- The decision structure, and
- The decision question

The researcher also anticipated that email is a generalizable example of the larger class of well-defined legacy systems.

The anticipated findings described above formed the basis of the research hypothesis. Specifically, the researcher hypothesized that

Hypothesis: *The US Federal Cloud Decision Framework (USFCDF) provides value to Federal IT decision makers in determining whether a well-defined legacy IT system should migrate to the Cloud.*

This primary hypothesis (aka ultimate probandum[3]) is further decomposed into two levels of sub-hypotheses (aka pentultimate probanda) :

Sub-hypothesis 1: The USFCDF decision factors[4] provide value to the Federal IT decision maker.

1a: All of the USFCDF decision factors are necessary.

1b: The set of USFCDF decision factors are sufficient.

Sub-hypothesis 2: The USFCDF decision structure provides value to the Federal IT decision maker.

2a: A decision structure provides value

[3] Ultimate probandum and pentultimate probanda are terms often employed by Wigmore to depict the higher echelons of an argument that marshals evidence in support of conclusions.
[4] Underlines represent the essence of the particular sub-hypothesis or subsub-hypothesis.

2b: The Value-Readiness paradigm of the USFCDF decision structure is useful for marshaling decision factors.

Sub-hypothesis 3: The USFCDF decision question is consistent with the needs of decision maker.

3a: The USFCDF decision question is consistent with US Federal guidance and regulations applicable to Cloud migration decisions.

3b: The USFCDF decision question consistent is with the needs of the decision maker.

These six subsub-hypotheses form six nodes at the lowest level of the Wigmore inference diagram, enabling more granular mapping of case study evidence to the hypothesis.

Limitations

The researcher is aware of the following limitations and, where appropriate, also describes corresponding mitigation actions:

- Decision process: The researcher does not intend to create a new decision process within the Federal agency, but rather to introduce the decision framework and associated decision factors to fit within the organizations existing IT governance process. The Federal agency may evolve its decision process to accommodate the new Cloud technology, but decision processes and further decision process evolutions are beyond the scope of this research.
- Efficacy of migration decision: This research only extends to the Cloud migration decision itself. The final linkage of the migration decision to the

subsequent performance of the system is also beyond the scope of this research. In other words, this research is about the migration decision at the time of the decision, and not as the decision might be viewed retrospectively after observing the legacy IT system operating within a Cloud environment. This research does not attempt to link decision factors to the subsequent success –or failure – of such migrations.

- Conflict of Interest (CoI): The researcher has clients who are Federal contractors and whose customers include all Federal agencies. To mitigate any perceived or actual conflict that may bias the researcher or the research, the following steps have, or will be taken:
    - Non-disclosure: Researcher will not disclose any information about the data source (Federal agency) to any client firms unless and until such information is published broadly. Should the data source become a topic of business conversation, the researcher will immediately announce the Nondisclosure and remove himself from the discussion.
    - Avoidance: Researcher will avoid data that could be used for advantage when bidding future business.
    - Conclusion: The researcher is investigating past actions and uncovering data on past decisions. The information from such activity will not likely provide any differentiated insight into any specific future government procurement. Given these actions, the researcher

does not feel there is a significant conflict of interest that would adversely affect this research project.

- Bias: Yin notes that "Case study investigators are especially prone to this problem [bias] because they must understand the issues beforehand". (Yin pg. 72) The researcher brings bias, conscious and subconscious, to this research. Conscious bias is the belief, based on literature and experience, that the USFCDF framework and decision factors are a close fit for a Federal agency making decisions about Cloud adoption. The researcher also is familiar to several Federal IT leaders, and the researcher may be perceived to be biased toward outcomes favorable personally to these two Federal leaders. To mitigate against known and unknown bias, the researcher proposes the following actions:
    - Establish criteria for case study selection in advance of actual case studies. In fact, the high-level criteria for the case studies in this research were previously approved (Proposal Addendum)
    - Provide transparency and auditability for all research.
    - Explicitly plan for construct validity, internal validity, external validity, and reliability in the research design. (Kider 1986)
- Construct validity: This research determined, in advance, the operational measures for the concepts being studies. This action guarded against subjective judgments in collecting data. Furthermore, the research design emphasized multiple sources of data such as separate corroborative interviews

combined with analysis of documents. All data collected for the research used a research repository and followed a pre-established chain of evidence.

- Internal validity: This research project links the use of several decision variables to the outcome of making a Cloud migration decision. The inferences between the two are supported through:
    - Documentation, as previously identified under the construct validity.
    - By using a predetermined framework from Kundra, which is the type of "logic model" advocated by Yin for internal validity. (Yin 2009)
    - Inferences were further supported through pattern matching, explanation building and exploration of rival hypothesis.
- External Validity: The findings of this research apply across all federal agencies. In other words, the results are can be generalized to other similar organizations. This generalization is supported by:
    - Adopting theory (i.e. Kundra's framework).
    - Using replication logic in a multiple-case study (Yin 2009)
- Reliability: The results of this research should easily be audited and even duplicated because of the reliability constructs built into the design and execution of the research. These reliability constructs include:
    - Establishing a case study protocol in advance of actual case study research
    - Disciplined employment of a case study database

The researcher feels that the scope of this research is appropriate and that the research design adequately addresses bias, construct validity, internal validity, external validity, and reliability.

Role of the Researcher

The researcher designed the research project, collected the research data, and analyzed the data to support the research findings.

Data collection, recording, and analysis instruments

The researcher applied several of the instruments applicable to qualitative research. Creswell lists the five prominent instruments for research data: (Creswell 2005)

- Observations
- Documents
- Interviews
- Audio-Visual
- Questionnaires

This research project employed four of the five instruments listed above (all but Audio-Visual). Note: In exploratory discussions with the data source (Federal agency) leadership, the agency leadership indicated that it would be appropriate to record interviews. Furthermore, the agency leadership felt that remote meetings were a viable method (e.g. Microsoft Live Meeting©) and that these session also could be recorded. Sound recordings were made of all interviewers.

Advocacy / Participatory Issue

Vivek Kundra, the former US Federal Chief Information Officer suggested a decision framework and a set of decision factors applicable for Federal agencies considering

adoption of Cloud. Although USFCDF remains poorly defined beyond a high-level description, they provide the best theoretical framework for evaluating a Cloud migration decision. Therefore, research proposing evaluation of the USFCDF suggests advocacy of the USFCDF. To guard against such a bias toward the Kundra framework and set of decision variable, the case study data collection, and particularly the interviews, were designed to gain insights on the decision framework and variables prior to questioning about the Kundra framework.

Anticipated Ethical Issues

This study poses no ethical issues.

Preliminary Pilot Findings

There is no evidence that the USFCDF has been piloted in a Federal agency. However, the researcher has presented the framework and decision factors to IT leaders in the DoD Joint Staff, to the members of the VA's Rapid Reduction Task Force (RRTF), at the Annual Air Force Information Technology Conference, and finally at a special FOSE Conference on Cloud computing. Feedback from these activities suggests that the framework and factors resonate with IT professionals in the Federal Government. Furthermore, initial conversations with VA IT leaders and participation as an observer on the VA RRTF indicate a positive response to these research questions.

Appendices Related to Research

This section will contain an overview of the appendices related to this research, to include:

- Interviewee Solicitation Letter
- Guidance to interviewee

- Researcher response form
- Background on each case study

CS Phase 2 – Research Design

The research design provides the logic that links the research questions to the data and associated conclusions. This step ensured the evidence collected addresses the initial research questions and therefore links to the research hypothesis. Thus, the research design phase is more about the logical challenge than the logistics challenge of the research.

This research project requires four activities for the case study design phase. (Yin 2009)

1. Define the unit of analysis (UOA) of the likely cases to be studied.
2. Develop theory, propositions, and the issues underlying the anticipated study.
3. Identify the case study design type and case selection criteria.
4. Define procedures to maintain case study quality.

Activity 1 - Define the unit of analysis (UOA) and the likely cases to be studied

Stake emphasizes the importance of getting the UOA right and uses the term quantain to describe the UOA for a single case (single case study) or a collection of cases (multicase study) (Stake 2006). Relating this to systems engineering, the UOA can be considered the equivalent of a systems context diagram because it defines the context and scope of the case study. The context is important for the case study much like it is for a system because the context defines the external boundary of the case and external interaction on the case. The scope of the case study might also been seen a rough parallel to the nature of a system in a systems context diagram. For example, any one of different types of

systems – manual, IT, or mechanical – could be used to produce a desired systems outcome. Similarly, different types of case study UOAs could be used to produce data and provide logical linkages to support findings related to the research questions. But, also like a systems engineering trade study, some UOA's are better suited for a particular problem than others.

To determine the appropriate UOA, the research first identified potential types of UOA's. Illustrative case study topics include individuals, small groups, organizations, partnerships, communities, relationships, decisions, and projects. (Yin 2009) For this research project, several types of UOA's could be eliminated easily because they provided only a limited relationship to Cloud migration decision. For example, individuals, partnerships, communities, and relationships do not link well to decisions about Cloud migration. That left a smaller set for further consideration: Small groups, organizations, projects, and decisions.

Small Groups: This UOA has merit because the decisions for Cloud migration were often made by small teams within a federal organization. Furthermore, by analyzing these teams, the researcher might gain insight into other interesting aspects of Cloud migration decisions, such as how the team operated, how they determined their decision factors, how they collected their data for the decision, and what expertise is required of such a team. However, most of these interesting aspects are external to the research question. Furthermore, it was not apparent that the Cloud migration decision was always made by a team instead of a single decision maker or a pre-established internal organization.

Organizations: Clearly, this case study is focused on Agencies within the Federal Government. By studying the Agency, or perhaps the IT organization within the Agency, the researcher would gain insight into the research problem. However, such organizations also handle many other activities other than Cloud migration decisions. Therefore, studying an Agency or an IT organization internal to the organization would be sufficient, but not necessary for this research.

Projects: Through exploratory inquiry, the researcher learned that once a Federal Agency decided to migrate to Cloud, they formed a project team for the migration. By adopting the project team as the UOA, the research project would likely uncover insights into the factors necessary for implementing a Cloud decision. However, the activity of the project team occurred post-decision – the project typically consisted of implementing the Cloud migration decision -- and therefore projects were not optimal for the UOA. This does not mean that the project team should not be consulted as they likely have evidential artifacts related to the prior Cloud decision itself.

Decisions: This brings us to considering the Cloud migration decision itself as the UOA. The decision consists of the decision factors, the framework used (if any), data supporting the decision factors, and the decision makers. Also, as mentioned earlier, the decision as the UOA or quantain has early roots in case study research. *Thus the Cloud migration decision itself is the best option for the UOA – as it provides the best combination of coverage and linkage to the research questions without adding unnecessary extra scope or complexity.*

Activity 2 - Develop theory, propositions, and issues

Although not absolutely required for case study research, the focus of the project and the strength of the resulting conclusions benefit from interleaving relevant theory as a foundation for the research logic. (Yin 2009) Similarly, Friedman and Sage describe "Pattern Matching" as one of two reasons for adopting a case study methodology. "Pattern matching contrasts and compares an empirically observed pattern with one that is predicted. This might be used, for example, to compare our case study to one found in the literature. Here a researcher develops a prediction about patterns expected to be seen in collected data. The associated analysis attempts to determine the pattern that best corresponds to observed data." (Friedman and Sage 2003) For this research project, the Yin's foundational theory and Friedman/Sage's predicted pattern is the USFCDF proposed by former Federal CIO Kundra. Specifically, this research project compared actual Cloud migration decisions to the USFCDF. (See Figure 21) The USFCDF itself benefits from alignment with the Technology Acceptance Model, a theoretical framework related to the adoption of new technology. The theory, prepositions and issues are further strengthened by adopting NIST's definitions for Cloud, to include the set of characteristics that determine what IT capabilities can be referred to as Cloud (and by inference, identify those that cannot claim to be Cloud), Cloud deployment models, and Cloud delivery models. And, to help link case study observations (aka evidence) to the overall hypothesis, Wigmore inference modeling was adopted as the inference diagraming standard and an inference modeling tool – Araucaria -- was employed to diagram the Wigmore inference diagrams. The next subsections describe the elements of

the adopted theory in more detail, to include: the three elements of the USFCDF, NIST definitions, and Wigmore modelling/diagramming.

USFCDF Decision Factors (DFs)

Kundra suggests a set of decision factors for federal Cloud-based IT capabilities. (Kundra 2010; Kundra 2011) Kundra suggested these decision factors for general decisions about federal Cloud capabilities. They apply to new development (aka green fields) as well as to legacy systems (aka brown fields). Because the more pressing issue is migration of legacy systems, (many more resources are applied to IT sustainment than IT development), this research focuses on decision factors for migrating legacy systems to Cloud.

USFCDF Decision Structure (DS)

A decision structure (DS) is a construct that helps a decision-maker by conceptually organizing related decision factors. A DS falls short of decision support model in that a DS makes no attempt to define the relationships between decision factors beyond high-level grouping. In particular, a DS does not provide quantitative relationships between decision factors within the framework as one would anticipate from a decision support model.

The overarching decision framework, which includes the DS, proposed for this research is based on what Kundra, the former US CIO proposed in his Federal Cloud Strategy. (See Figure 30) This framework was recommended by a committee of industry and government IT leaders assembled under the auspices of a nonprofit association.

This framework categorizes decision factors into two groups; those related to the value of adopting Cloud, and those relating to the readiness for migrating a system to Cloud.

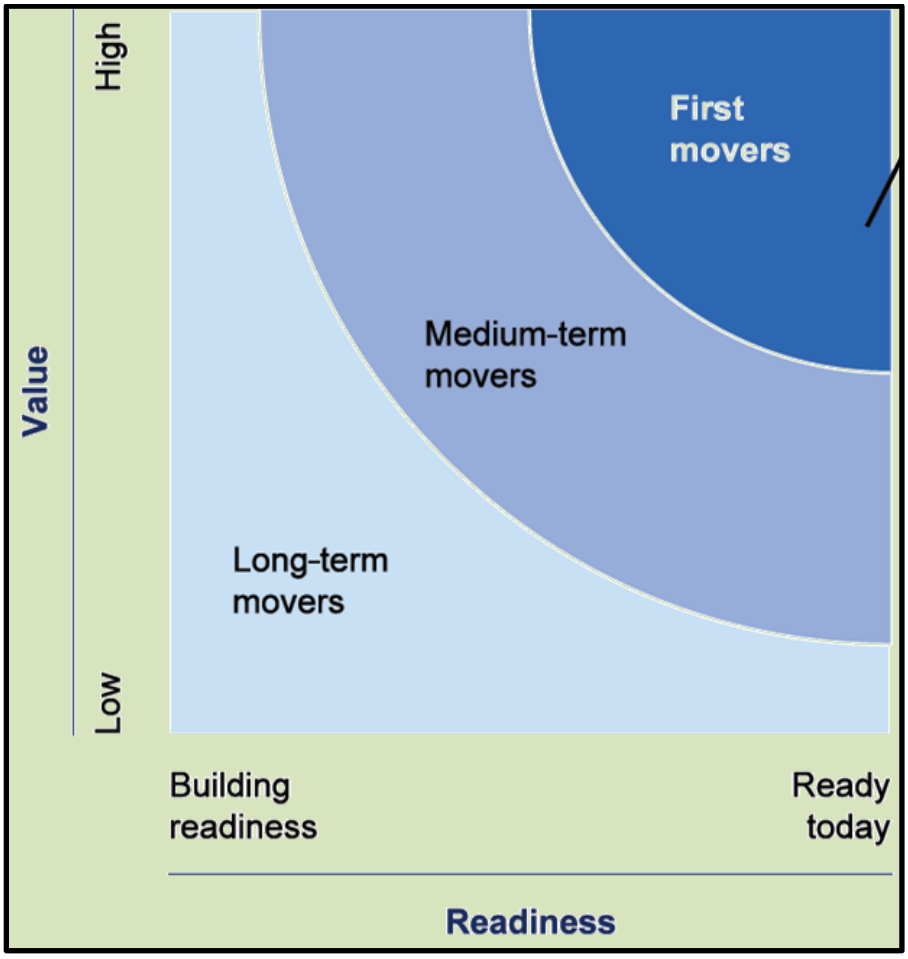


Figure 30 - Federal CIO Proposed Decision Structure

This DS of the USFCDF is congruent with a family of technology acceptance models (TAMs) that use similar groupings. The most common TAM uses the term feasibility to describe factors related to readiness. Readiness and feasibility have similar meanings, but readiness implies a temporal aspect to feasibility. Readiness implies that even if an

organization might not find migration to Cloud feasible now, that they may find the same system feasible for migration in the future as the situation changes. Another similarity of TAM and Kundra is that the feasibility/readiness category acts as a governor, limiting the ability of an organization to take action on what otherwise would be a decision of value to the organization.

The topic of Cloud in general is relatively new. Cloud migration within Federal agencies is even more immature. Therefore the current level of Cloud migration decisions does not currently support a quantitative decision model. Rather, Federal agencies today would better value an organizing construct which a framework provides to help them conceptualize their decision about Cloud migration. Furthermore, the Kundra-based framework is consistent with the widely accepted model for technology adoption decisions. Therefore, the framework evaluated in this research will be the Kundra Value-Readiness framework.

USFCDF Decision Question (DQ)

The decision question represents what it is that the decision maker should answer. In USFCDF, the general problem is to "Identify which IT services to move and when." (Kundra 2011) This implies that the decision for each specific legacy IT system is to decide whether that system should migrate to the Cloud. The USFCDF DQ therefore appears as a binary decision – migrate or do not migrate. This is consistent with prior work (mostly surveys) that investigate the considerations for deciding whether a system should migrate to the Cloud. This research project includes investigation into whether the USFCDF DQ is consistent with the DQs needed to make actual Cloud

migration decisions in the Federal Government. For example, Federal Acquisition Regulations and other guidance affect decisions like Cloud migration because they involve procurements – contract agreements to spend Federal dollars. (AT&L 2003)

NIST Cloud Definitional Theory

This research also leverages theory and adopted standard definitions published by the US National Institute of Standards and Technology (NIST) to provide the rationale for bounding the case quantain. NIST provides three aspects of Cloud theory and definitions relevant to bounding the quantain:

1. Cloud characteristics, defining what constitutes a valid Cloud migration decision
2. Cloud Deployment Model, describing the nature of the Cloud service within the NIST Cloud hierarchy
3. Service Delivery Model, which characterizes the type of Cloud migration based on the relationship between the Federal Agency making the decision and the type of Cloud provider targeted for the migration

NIST provides definitional theory describing the characteristics of Cloud. In other words, NIST provides a means of determining whether an IT capability can be considered to be of a Cloud type. These characteristics are described in detail in Chapter 2, Section One – Cloud Characteristics. (page 19) NIST provided five characteristics defining Cloud: (NIST 2011)

- *On-demand self-service*
- *Broad network access*

- *Resource Pooling*
- *Rapid elasticity*
- *Measured Service*

This research project will use this definitional model to limit the target case studies to those IT migration decisions having a target migration type consistent with all five of NIST's Cloud characteristics. This rigor is important because some Federal IT implementations depicted as Cloud by Federal Agencies arguably failed the NIST criteria for Cloud. An analysis of the first 78 Federal Cloud implementations across the Federal Governments suggests that as many as a third of Federal IT deployments credited as Cloud implementations did not provide evidence to support the target type as Cloud. For example, several of these systems reflected only web-enablement of an existing legacy client-server system which, by nature of web-architecture, leveraged broad network access, but lacked aspects of the other four defining characteristics. (Mink 2011)

Cloud Service Delivery Models – NIST identifies three types of services offered by a Cloud IT implementation. In addition, the researcher suggests two additional service types consistent with NIST definition of Cloud characteristics. These characteristics are described in detail in Chapter 2, Section Two – Cloud Service Delivery Models. (page 24) The three NIST defined service delivery models include:

- *Software-as-a Service (SaaS)*
- *Platform-as-a-Service (PaaS)*
- *Infrastructure-as-a-Service (IaaS)*

These three service delivery models are generally considered hierarchical in that IaaS consists primarily of the lower-level computing hardware and operating systems, PaaS builds on IaaS with middleware, and SaaS builds on IaaS to deliver functionality to the user. SaaS generally provides the most functionality; is the most differentiated from a legacy system, and encapsulates the issues and characteristics of PaaS & IaaS. Therefore, this research project will be constrained to decisions related to legacy IT systems migrating to SaaS. This will provide the richest and most generalizable results while eliminating one set of variables among the cases being studied.

Cloud Deployments Models – NIST identifies four ways Cloud services can be offered to an Agency. . These four deployment models are described in detail in Chapter 2, Section Three – Cloud Deployment Models. (page 35) The four NIST defined deployment models are:

- *Public*
- *Community*
- *Private*
- *Hybrid*

Preliminary literature study indicates that early Cloud decisions involved only two of these deployment models – public and community. Decisions regarding private clouds were relatively rare in the Federal space because, by definition of this deployment model, the Cloud provider and the Cloud consumer were one and the same Federal Agency (Mink 2011) Such a deployment model provided limited economies of scale and therefore limited benefits to the agency compared to other deployment models. This

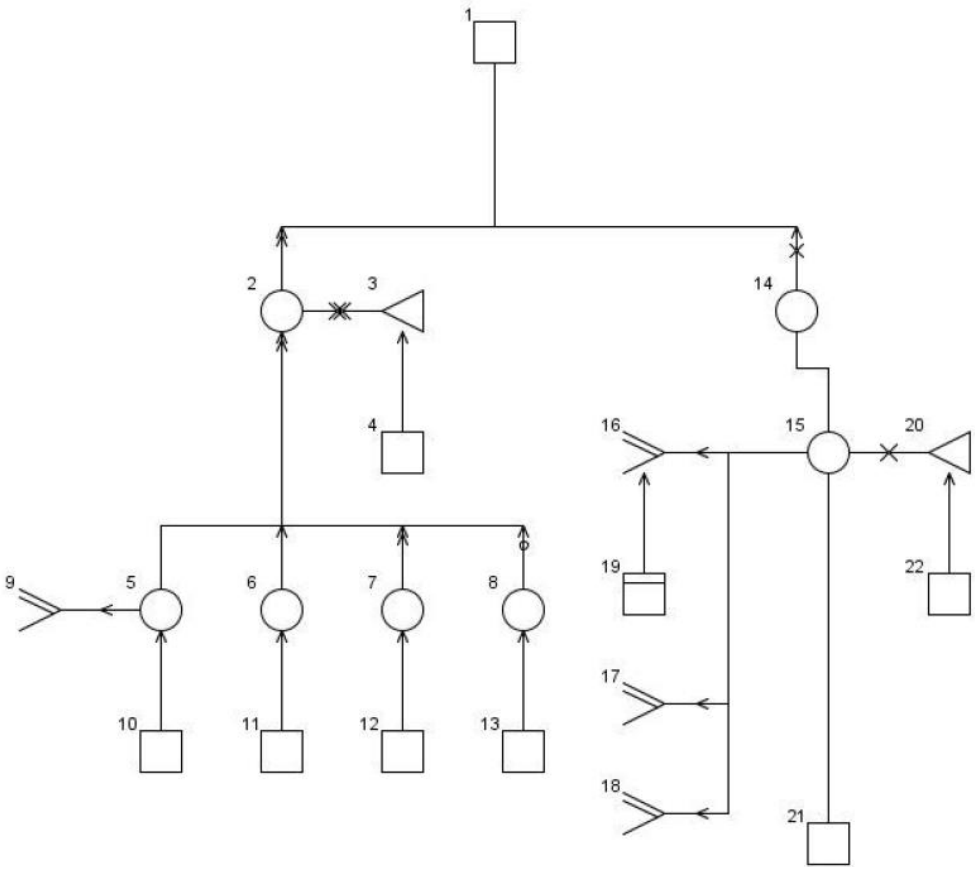
research project will exclude hybrid deployment models because, by definition, they combine public and private clouds and would therefore introduce uncertainty as to whether one or the other component deployment models – or their combination – affected the migration decision. NIST definitional theory shapes this research by constraining decisions to those considering migration to a public or community Cloud deployment model.

Wigmore Inference Diagraming and the Araucaria Tool

This research project adopts Wigmore inference diagrams and applies the Araucaria diagramming tool to explicitly link the case study evidence to the overarching hypothesis (aka penultimate probanda). This Wigmore structural construct enables this research project to overcome one of the challenges of case study research, which is marshalling case study evidence to provide convincing support for the research conclusions.

John H. Wigmore developed a graphical and analytic structure integrating the relevance, credibility, and probative forces of evidence. (Wigmore 1937) Joseph Kadane and David Schum endorsed Wigmore's inference structure in their treatise exploring the evidence and conclusions surrounding the famous Boston trial of Sacco and Vanzetti. (Kadane 1996) Case studies, like trials, are difficulty because they both involve probabilistic judgments about evidence and require a means of ensuring the researcher and readers are all on the same page. According to Kadane and Schum, "Wigmore's methods allow us some effective ways of managing this difficulty." The remainder of this section summarizes Wigmore methods and introduces the XML-based tool used to create the Wigmore diagrams used in this research project.

Wigmore diagrams use a box and arrow structure, linking primary evidence through intermediate levels of evidence, ultimately linking to the primary hypothesis. These evidentiary levels are sometimes referred to as statements in a Wigmore diagram. One strength of Wigmore diagrams is that Wigmore's method constrains and classifies the various levels of statements and the inferences that link them together according to their roles in supporting or disputing conclusions in a court case. The statements may be affirmatory or negatory, arguing for or against another statement. Furthermore, each linkage between statements relate the force, or strength, of the linkage – ranging from "no effect" to "very strong." Glenn Rowe and Chris Reed, the creators of the Wigmore diagraming tool "Araucaria," provide an excellent sample diagram and associated description (see Figure 31).



Node 1 is the conclusion which the prosecution is attempting to prove. In the diagram, square nodes are testimonial evidence, circular nodes are circumstantial evidence, nodes with > symbols (such as nodes 9, 16, etc.) are explanatory and closed triangular nodes (such as nodes 3 and 20) are corroborative evidence. Nodes with a double line near the top (9, 16, 17, 18 and 19 in Figure 1) are defendant's evidence; all other nodes are prosecution's evidence. In this diagram, therefore, the prosecution is putting forward most of the evidence and the defense is providing explanatory evidence to counter the prosecution's argument at nodes 5 and 15. The various symbols on the support arrows indicate the degrees of support. A single arrow indicates the direction of support, so that node 19 supports node 16, for example. A double arrow, such as from nodes 2 and 7, indicates strong support. The arrow on the edge between nodes 16 and 15 indicates that node 16 detracts from the support to node 15, which is to be expected since node 16 is explanatory and attempts to lessen the effect of node 15. The X on the edge between nodes 15 and 20 indicates that the corroborative node 20 supports node 15. The small circle on the edge leading out of node 8 indicates a negatory force, so that node 8 detracts from the support to node 2. The double arrow just below node 2 indicates the net probative value of nodes 5, 6, 7 and 8.

Figure 31 - Sample Wigmore Diagram (above) and Associated Description (below). (Rowe 2006)

For this research project, the researcher attempts to operate in an unbiased fashion, to include observations that detract from supporting the hypothesis (negatory forces), along with collaborative observations that offer insights into the related negatory forces. In courtroom terms, the researcher plays the role of the prosecutor and defense in marshalling evidence related to the hypothesis.

As noted by several authors, to include Kadane and Schum, Wigmore diagraming is detailed and expands rapidly. The diagrams often must be blocked into sections so that the whole picture and the corresponding depth can both be depicted. Fortunately, two researchers, Chris Reed and Glenn Rowe, both at the University of Dundee, developed a tool they named Araucaria to display three forms of inference diagrams, including Wigmore diagrams. (Reed 2004) Araucaria enables researchers to create Wigmore diagrams and also convert to and from Wigmore into other forms of inference diagrams while retaining concordance. Because Araucaria stores its internal data in a form of eXtensible Markup Language (XML), detailed editing of Araucaria's Wigmore diagrams is possible through a separate external XML editor. This research project benefited from adopting Wigmore diagrams and related tools to support the conclusions in the subsequent chapters.

Activity 3 - Identify the case study design type and case selection criteria

The case study design type for this research is the multicase study. The rationale for this design type is described and supported in Chapter 3, Analysis of Competing Research Methodologies (page 90). One key challenge in designing the multicase study is determining n, the number of cases to be studied. Yin notes that good case study research

supports “analytic generalization,” which links cases study conclusions with theory. (Yin 2009) He contrasts analytic generalization from “statistical generalization.” Statistical generalization makes an inference about a large population based on a sampling, usually randomly chosen, of the population. Analytic generalization, in contrast, carefully selects the objects of study and identifies insights that support the linkage between the cases and the associated theory. By carefully selecting cases with similar characteristics – literal replication – conclusions can be reached with a few cases (2-3). Should the cases vary in some characteristics, which is nearly always impossible to preclude, then additional cases or partial cases may be required to fully support common findings and explain any variations in findings.

Non-varying Case Characteristics (Replication Logic)

Following the recommendations of Yin, this research project will set n=3 for replication logic, based on an initial assumption of nearly identical contexts for the case studies. Then additional partial cases are added to account for variances from literal replication among those three cases. This research project will adhere to replication logic except for pre-identified variations to adequately answer the research questions. As described earlier, the following characteristics of the cases will be held constant:

- The Unit of Analysis (quantain) will be a Cloud migration decision.
- The IT system for the quantain will be a *legacy* IT system migration.
    - Note, this specifically excludes new IT Cloud capabilities (developmental projects).

- The type of Cloud service delivery model will be Software-as-a-Service (SaaS).
    - Infrastructure and Platform-as-a-Service are excluded.
- The SaaS IT Capability will be messaging and collaboration, specifically Email as a Service (EaaS).
    - Other SaaS services are excluded.
- The organization making the decision will be a US Federal Agency.
    - Other types of organizations, such as private firms, nonprofits, lower-level US governments (i.e. state & local) and foreign government agencies are excluded.
- The theory will be based on Kundra's Cloud migration decision framework.
    - This guides the research and case selection to the extent that the case's framework and decision factors can be related to the Kundra framework and decision factors.
-

Variations from Replication Logic

As noted by Friedman and Sage, "it will often be the minimum essential set of measurements and data that most clearly illuminates the workings of the newly investigated phenomena." (Friedman and Sage 2003)

However, this research requires some case characteristics to vary because of the nature of this research problem and associated research questions described earlier. (see Problem

Statement, page 100) The research problem and associated questions drive the cases to vary in the following two characteristics:

1. Size of the IT system migrating to Cloud. This study attempts to identify whether the study can be generalized to both large and small migrations. Therefore this research will include a case or partial case for a large as well as a small migration.
2. Nature of Federal Agency mission. This study attempts to identify whether the study can be generalized across all Federal Agencies, including both civil and national security agencies. Therefore this study will include at least one civil agency case and at least one national security agency case.

These two variations from literal replication (deployment model, migration size, and federal agency mission) merit further discussion.

The first variant from the literal replication is the size of the Cloud migration. A significant trend in Federal IT acquisition is the move toward smaller, more modular "chunks" of IT Capability. Cloud supports such an incremental and modular approach. Therefore, it's likely that most Cloud migration decisions will involve projects smaller than the original (prior) investment for legacy systems themselves. However, like the previous discussion about deployment models, Federal Agencies will migrate modest as well as larger IT capabilities to Cloud. Therefore, to support research findings across the spectrum of legacy systems in the Federal Government, this research will investigate at least one large and at least one small system migration. Investigating smaller and larger migrations will ensure relevancy while also helping inform the results. For this research

project, a large migration is defined as a decision to deploy a Cloud capability affecting over 100,000 users or costing more than $40M. This threshold for a large-size Cloud migration in terms of users or migration costs, is a significant impact and investment. These thresholds also align with existing characterizations of Federal Agencies and IT acquisition efforts.

Users (100K users): The US Federal Government classifies the top-level of Federal Agencies (often the Department level) into four size categories: large, mid-size, small, and very small. (DoJ 2001) The large category is for Agencies with 10K or more employees. Eighteen agencies belong to this category. Of those 18, only 7 have 100K or more employees. There is a sharp drop (by a third) below the 100K threshold within the large category. This supports the user definition (of 100K) used in this research project to categorize the size of a Cloud migration as large.

Cost ($40M): The US Government (DoD in particular) characterizes IT investments as Major Automated Information Systems (MAISs) if their costs are estimated to exceed $40M in a given year. (USD(AT&L) 2008) A MAIS belongs to the second highest acquisition category among the four DoD acquisition categories for all acquisitions, including new weapons systems. This supports the cost definition (of $40M) used in this research project to categorize the size of a Cloud migration as large.

Large IT system migrations are those that meet or exceed either the user or the cost thresholds defined above for the large category. IT system migrations not reaching either of those thresholds are characterized as modest for this research project. The research plan includes research into both large and modest migrations.

The second variation from literal replication is the nature of the mission of the Federal Agency. As of the time of this research project, the US Government's own online reference lists 456 separate Federal Agencies. (USG 2012)[5] Each agency has a unique mission. The largest agency in terms of budget and employees is the Department of Defense (DoD), which in turn, has subordinate agencies such as the Department of the Army, Defense Information Systems Agency, etc. The DoD's focus on national security has raised questions about the security of the Cloud. Mark Orndorff, DISA Program Executive Officer for Mission Assurance emphasized this concern and sought insights from industry during a one-day technical exchange on DoD Cloud Security. (Orndorff 2010) Also, initial survey-based research by the Air Force Institute of Technology (AFIT) titled appropriately titled "I Can, but I Won't: An Exploratory Study of People and New Information Technologies in the Military" indicated that Defense IT leaders differed from leaders in other organizations in their view of the viability of Cloud migration. (Killaly 2011) Furthermore, DoD needs to be included in a study of Federal Agencies because DoD spends more for IT and has more IT systems than any other Federal agency. (Kundra 2011) Therefore, to support generalization and to identify situations where factors diverge across agencies, this research project will include at least one case from a DoD agency and at least one case from a non-DoD agency.

The researcher evaluated DoD as a source of research data by personally discussing the research project with each of the following DoD IT Leaders. (by position, not name)

[5] Note, the US Government counts the number of Federal Agencies different ways at different times, sometimes resulting in conflicting numbers from differing official USG sources.

- DoD CIO
- DoD Deputy CIO
- Army CIO/G6
- Army Chief of Data Center Consolidation
- Air Force Deputy CIO
- Air Force Program Executive Officer for Business Enterprise Systems
- Air Force Electronic Systems Center Executive Director
- Air Force Space Mobilization Augmentee to A6
- Defense Information Systems Agency (DISA) CIO

One final note about diversity of the Federal Agency; some may argue that diversity among Federal Agencies selected for the cases reflects diversity across contexts rather than variations in replicative logic. Such diversity is seen as positive and is one of the three selection criteria listed by Stake. (Stake 2006) But, regardless of whether diversity in selection of Federal Agencies is considered a variation from replicative logic or simply good sense for diversity across contexts, both rationales support the need to include at least one DoD and one non-DoD agency.

Other considerations for case study selection criteria

Thus far we've discussed two groups of selection criteria for case study selection:

- Criteria related to replicative logic
- Three Criteria that varied from replicative logic

These two groups were carefully researched and selected, a priori as to provide rigor and strongly support research findings.

However, these case studies involve real agencies whose leadership and formal guidelines affect their suitability for study. Therefore, there is a pragmatic element to case study selection; access to pertinent decision makers and related decision data. As described earlier in the discussion about case study planning, each full case study requires triangulation of at least three source of case information (usually consisting of interviews or documents). This eliminates cases where the Federal Agency declines participation. This also eliminates cases where the decision maker(s) are no longer available. This also eliminates cases where the decision makers are reluctant to share information about the Cloud migration decision. If the decision maker feels that this research project might cause embarrassment personally or to the agency, he or she would be reluctant to participate in the research.

To encourage participation and keep the research scope feasible, the research project was purposefully constrained to explore only data related to the decision itself, and not to the efficacy of the decision or to the quality of the actual migration itself. In other words, the researcher defers to later research projects conclusions about what factors surrounding the migration decision relate to the subsequent success (or failure) of the actual migration.

The research also leveraged the credibility of the research and the GMU advisory committee to help persuade the Federal Agency decision maker(s) to agree to support a case study based on their Cloud migration decision. Although not an explicit selection criterion, the research team's reputation and associated existing relationships helped obtain cases for research.

Stake and Yin both concur with this pragmatic criterion. Stake notes that he "usually favors cases from which we can learn about their activity and situation. This may mean taking the ones that are most accessible, the ones we can spend the most time with." (Stake 2006)

Case Study Candidates

Table 9 summarizes the case studies selected for the research plan.

Table 9 - Case Study Candidates

Case		Replicative Logic Constants				Planned Variations	
Agency	Full/ Partial	Cloud Migration Decision	Legacy IT System	Delivery Model (SaaS/ EaaS)	Relatable to Theory	System Size	Agency Type
Army	Full	✓	✓	✓	✓	Large	DoD
NSF	Full	✓	✓	✓	✓	Modest	Non-DoD
VA	Full	✓	✓	✓	✓	Large	Non-DoD
GSA	Partial	✓	✓	✓	✓	Modest	Non-DoD
USAID	Partial	✓	✓	✓	✓	Modest	Non-DoD

The cases selected conform to the study design criteria described earlier; specifically that these cases provide three full case studies and two partial cases studies; all conform to the replicative logic; and provide the proscribed variations to explicitly explore insights that engender generalization necessary to address the original research problem as well as the associated research questions.

Activity 4 - Define procedures to maintain case study quality

This research project will ensure case study quality through application of:

- Construct validity

- Internal validity
- External validity
- Reliability

Construct validity: This research determined in advance the operational measures for the concepts being studies. This action guarded against subjective judgments in collecting data. Furthermore, the research design emphasized multiple sources of data such as separate corroborative interviews combined with analysis of documents. All data collected for the research used a research repository and followed a pre-established chain of evidence.

Internal validity: This research project links the use of several decision variables to the outcome of making a Cloud migration decision. The inferences between the two are supported through:

- Documentation, as previously identified under the construct validity.
- By using a predetermined framework from Kundra, which is the type of "logic model" advocated by Yin for internal validity. (Yin 2009)
- Inferences were further supported through pattern matching, explanation building and exploration of rival hypothesis.

External Validity: The findings of this research apply across all federal agencies. In other words, the results are can be generalized to other similar organizations. This generalization is supported by:

- Adopting theory (i.e. Kundra's framework)
- Using replication logic in a multiple-case study (Yin 2009)

Reliability: The results of this research should easily be audited and even duplicated because of the reliability constructs built into the design and execution of the research. These reliability constructs include:

- Establishing a case study protocol in advance of actual case study research
- Disciplined employment of a case study database

The researcher feels that the scope of this research is appropriate and that the research design adequately addresses bias, construct validity, internal validity, external validity, and reliability.

CS Phase 3 – Preparing to Collect Case Study Evidence

This phase develops the case study protocol and gains approval for the human subjects' protection. The activities for the action taking phase consist of:

Activity 1) Individual case study protocol. (the procedures to follow for each case)

Activity 2) Human subjects protection. (procedures to follow when interviewing people)

Activity 1 – Individual case study protocol

The case study protocol contains the collection plan as well as the procedures and general rules to be followed in researching the case. The protocol promotes the reliability of the case study, particularly for a multicase study such as this research project because it promotes consistency among the cases researched. (Yin 2009) For this research, the case study protocol consisted of these steps and associated research artifacts for each case and partial case study:

1. Research the agency and the Cloud migration.
    - Using open source information.
2. Identify senior sponsor within the agency.
    - Employing literature study and prior informational interviews.
3. Formally request support from the agency sponsor.
    - Using previously prepared introductory email.
    - Preceded by an informal verbal inquiry if possible to increase likelihood of acceptance.
    - The sponsor's response identified candidates for case study interviews to include the agency's decision maker.
4. Prior to each case study interview schedule and prepare the interviewee with a read-ahead package providing background.
    - Using a previously prepared read-ahead email
5. During each interview, initially baseline the interviewee about the purpose of the research, the interview structure, and interviewee rights.
    - Using slides prepared in advance (see Figure 32).

Figure 32 - Consistent baselining at the initiation of each interview

- The baselining grounds the interviewee in the Kundra framework that guided the subsequent interview. During baselining, the researcher also confirms that the interviewee is comfortable with recording the interview and determined whether the interviewee would permit the researcher to attribute their comments to them by name – i.e. verification of attribution or confidentiality.

6. After initial baselining, the researcher interviews the interviewee
   - Using a standard collection template, augmented by reference to definitions in the previously presented background slides.
   - The standard collection template followed a standard flow:
     - Context of the migration (legacy system, decision timing, decision process, decision makers, etc.).
     - Investigation into value decision factors.
     - Investigation into Readiness decision factors.

        - Open ended questions, to include inquiries about other sources of data such as additional interviewees and associated records.
    - The researcher captured written notes and, when allowed, audio recording as well.
7. After each interview, the researcher transcribed the interview for later reference.
    - Each interview spanned between one hour to three hours depending on the style of the interviewee's dialog and the amount of information the interviewee could convey.
    - The research also sent a follow-up note of appreciation following each interview

Following is the analysis of each interview, as well as the analysis of all interviews.

Activity 2 – Human Subjects Protection

This research project interviews IT decision-makers and their staff relevant to the Agency decision to migrate a legacy IT system to Cloud. To ensure this research project complied with federal, state, and university requirements, the researcher submitted the research protocol (#7946) for review. The GMU Office of Research Subject Protections reviewed the protocol and determined it was acceptable and did not require further review by the Human Subjects Review Board since the research did not meet the federal definition of human subjects research. (Motsing 2012)

CS Phases 4-6 – Collecting, Analyzing, and Sharing

This research project follows Yin's six-phase case study methodology. The first three phases (Planning, Design, and Preparing) were described earlier in this chapter about research methodology. Table 10 provides a concordance depicting the first three phases as well as the remaining three phases, mapping all of Yin's six phases to this dissertation.

Table 10 - Mapping of Yin Case Study Methodology to this Dissertation

Yin Case Study Phase	Corresponding Dissertation Mapping
1) Planning	Chapter: 3 - Research Methodology Section: Planning
2) Research Design	Chapter 3 - Research Methodology Section: Research Design Section
3) Preparing	Chapter 3 - Research Methodology Section: Preparing to Collect Case Study Evidence
4) Collecting Case Study Evidence	Chapters 4-7 – <Individual Case Study Findings>
5) Analysis	Chapter 8 – Synthesis of Multiple Case Study Findings Chapter 9 – Conclusions
6) Sharing	Dissertation Publication, Articles, and Conference Presentations

The majority of the research project is in Yin's Phase 4, which comprise chapter 4 of this paper. Yin's Phase 5 (chapters 5 & 6 of this paper) analyze the findings to answer the research questions and support the project's hypothesis.

4. CASE STUDY FINDINGS

Introduction

This chapter summarizes the findings the five cases. As seen in Table 11, the research spanned three full cases and two partial cases. Full cases met the criteria by Yin and Strake for triangulation through multiple diverse sources. The partial case studies were less robust, but provided insight support generalization of the findings across different types of agencies (DoD and non-DoD) as well as across different system sizes (large and modest). For each case – full and partial -- the quantain defining each case was the decision by the Agency to migrate their legacy email system to a Software-as-a-Service (SaaS) Cloud delivery model and the research compared the decision to the US Federal Cloud Decision Framework (USFCDF) as a unifying theory for case consistency.

Table 11 - Summary of Research Case Studies

Case		Replicative Logic Constants				Planned Variations	
Agency	Full/ Partial	Cloud Migration Decision	Legacy IT System	Delivery Model (SaaS)	Relatable to Theory	System Size	Agency Type
Army	Full	✓	✓	✓	✓	Large	DoD
NSF	Full	✓	✓	✓	✓	Modest	Non-DoD
VA	Full	✓	✓	✓	✓	Large	Non-DoD
GSA	Partial	✓	✓	✓	✓	Modest	Non-DoD
USAID	Partial	✓	✓	✓	✓	Modest	Non-DoD

Each of the five case study summaries in this chapter follows an identical flow.

- Concise introduction of the case
- Answers to the five research questions/sub-questions (see Table 12) This section comprises the vast majority of the case study summary.
- Other findings and observations discovered during the research project that relate to the general research topic.
- Conclusion summarizing the findings from the case

Table 12 - Research Questions and Sub-questions

Main Body of Each Case Study Summary
1. Do the USFCDF decision factors provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?
a. Are all USFCDF decision factors necessary?
b. Is the set of USFCDF decision factors sufficient?
2. Does the USFCDF decision structure provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?
a. Does a decision structure (in general) provide value?
b. Is the Value-Readiness paradigm of the USFCDF decision structure useful for marshalling decision factors?
3. Does the USFCDF decision question provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?
a. Is the USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions?
b. Is the USFCDF decision question consistent with the needs of the decision maker?
4. Is email a well-defined legacy IT system?
a. Are email systems in the Federal Government defined by a small set of similar legacy commercial products?
b. Is email used across the Federal enterprise?
5. Would Cloud migration decision-makers have benefited from prior-knowledge of a validated USFCDF?

The remainder of this chapter summarizes each case in the order listed in Table 11 (i.e. starting with the Army) using the flow just described above. For additional background on each of the case studies, see the appendices of this report.

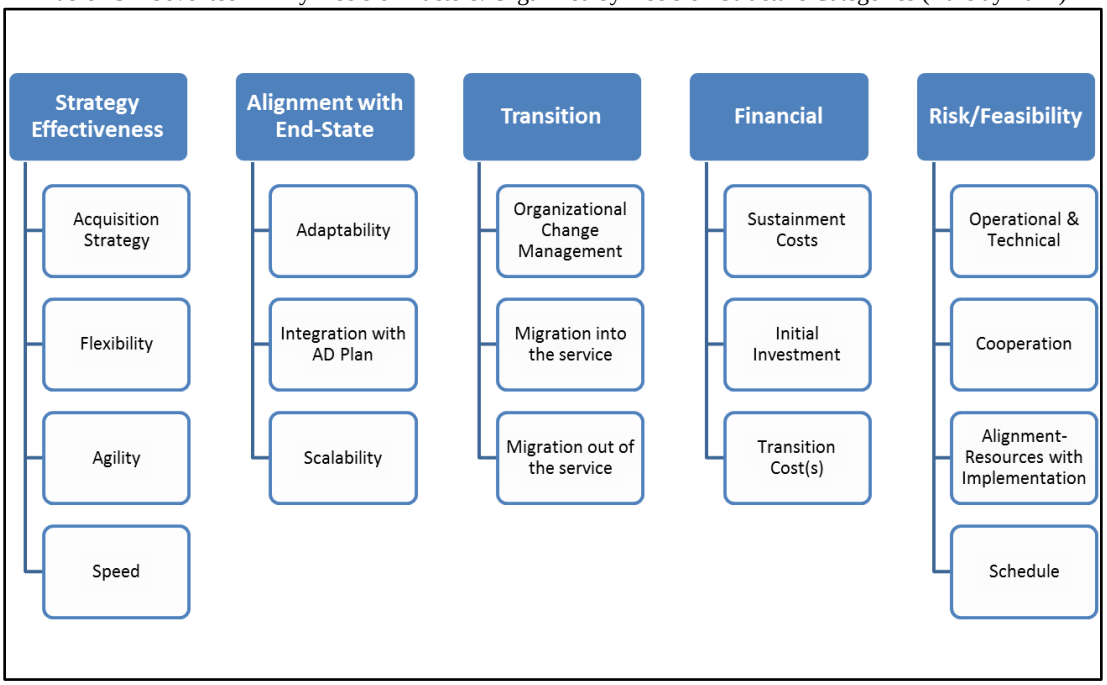
Case 1 - Army Enterprise Email

This case researched the 2010 decision by the Department of the Army to migrate their legacy email systems to a DISA cloud service initially named Army Enterprise Email (AEE) and subsequently renamed Defense Enterprise Email (DEE). AEE used Software as a Service (SaaS) for their cloud delivery model (see Chapter 2) and Community Cloud as their deployment model (see Chapter 2). Lieutenant General Jeffrey Sorenson, Army CIO and G6, led the decision making process and served as senior decision maker. The investigations for this case followed the methodology described in Chapter 3. The Army's champions for this case study research were Lt General Susan S. Lawrence, successor to LTG Sorenson as Army CIO and G6, and her deputy, Mr. Michael E Krieger. This case benefited from multiple investigative sources including: LTG Sorenson, Lieutenant Colonel Peter Barclay (Project Team Lead), internal Army documentation surrounding the decision, and numerous external publications surrounding the decision. The next sections summarize the findings and observations from this case study. See the appendices for more background and context on this case.

Q1 - Do the USFCDF decision factors provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The Army developed an explicit set of seventeen DFs organized into a five-category decision structure as depicted in Table 13.

Table 13 – Seventeen Army Decision Factors: Organized by Decision Structure Categories (Barclay 2012)



These seventeen Army DFs are defined in Table 14 on the next page.

Table 14 - Army Decision Factors: Definitions(Army 2008)

#	Decision Factor	Definition
1	Acquisition Strategy	Ability to quickly and efficiently deliver best value for an enterprise service. Balances the need for competition with other key considerations.
2	Flexibility	Ability to quickly enhance functionality based on operational needs
3	Agility**	Responsiveness, the ability of the COA to quickly insert capability based on new technology
4	Speed**	The quickness at which the a COA could be implemented
5	Adaptability	Ability to evolve the capability to joint environment
6	Integration with AD Plan	Supports the Army's [planned] consolidated Active Directory (AD) architecture [of Army personnel and other resources].
7	Scalability	Scalable to 5.3M users
8	Org Change Management	Level of effort in socializing the COA as viable, valuable, and productive
9	Migration – Into the service	Level of Effort in migrating a user into the service from existing
10	Migration – Out of the service	Level of Effort in migrating a user from the service to the end state [for Army future enterprise]
11	Sustainment Costs	Annual support labor, admin, facility, bandwidth, backup, and tech refresh costs (O&M)
12	Initial Investment	Upfront investment to stand up and enable the [transition to Cloud] with the stated [initial] capacity and message transfer
13	Transition costs	Cost required to migrate [initial] users to the COA
14	Operational & Technical Risk	Risk that COA will not meet requirements or operational needs of stakeholders
15	Cooperation	User acceptance of COA and Senior leadership buy-in
16	Alignment – Resources with Implementation	Risk the funding stream will not support the COA implementation plan
17	Schedule	Risk of COA meeting milestones and decision points

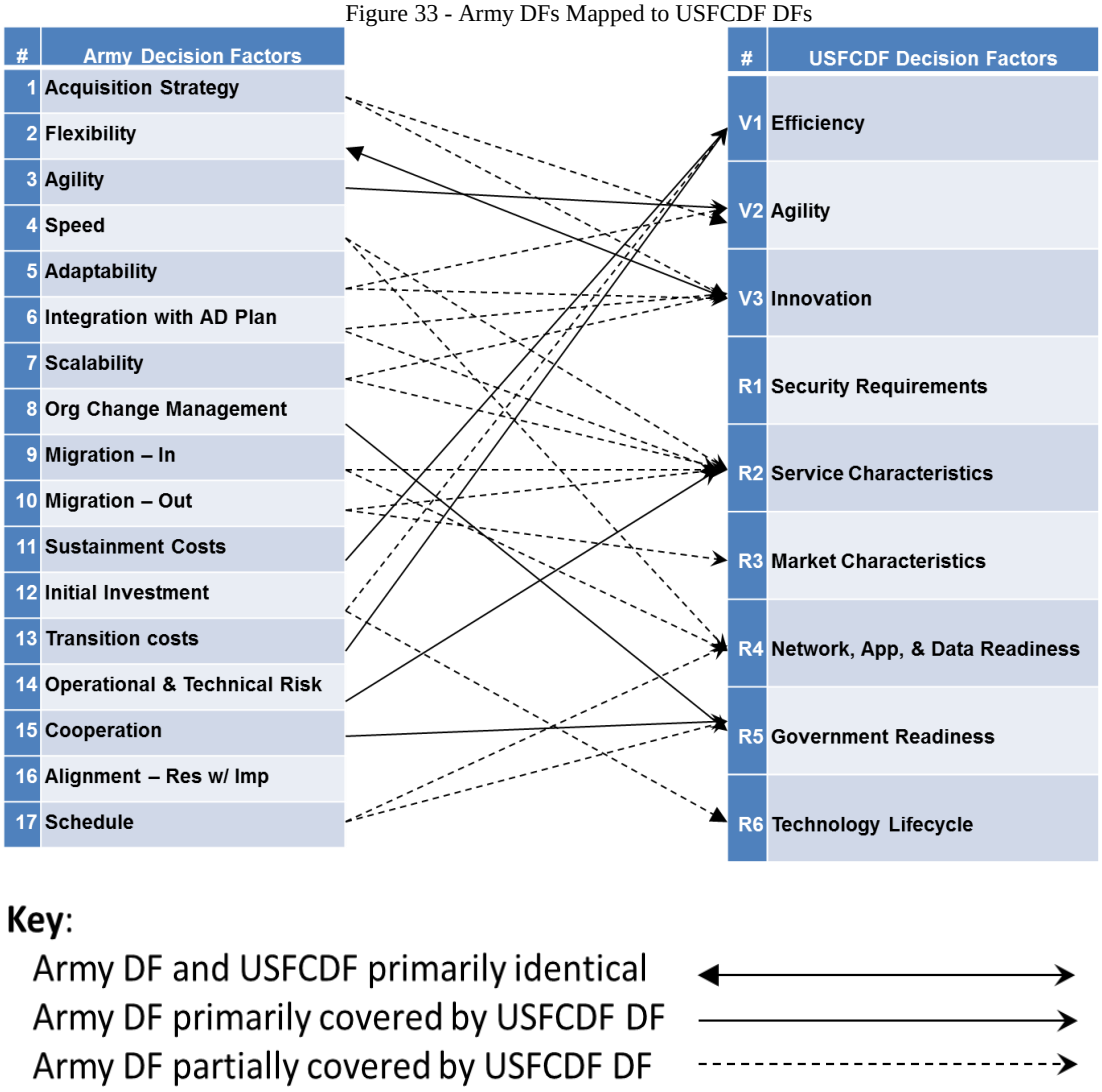
** COA – Course of Action (e.g. a specific option or alternative such as a going to Cloud)*
*** Army revised the initial set of DFs in 2010, adding Speed & Agility. (Barclay 2012)*

To answer question 1, the researchers compared the seventeen DFs used by the Army (see Army DF definitions above) to the nine USFCEF DFs described in Chapter 2 (listed on the right side of Figure 33). This comparison, along with other supporting evidence, was used to determine whether the USFCDF DFs were necessary and sufficient for a Cloud migration decision.

Q1a - Were all of USFCDF Decision Factors necessary for the Army decision?

All of the USFCDF DFs would be found necessary if the Army applied each and every one of them in their Cloud migration decision. Because the Army used a different set of DFs from the USFCDF, the Army DFs were mapped to the USFCDF DFs – as depicted in Figure 33.

Figure 33 - Army DFs Mapped to USFCDF DFs



The arrows in Figure 33 designate, for each Army DF, the corresponding USFCDF DF(s). A double line suggests a near-identical correspondence – one to one. A one-way solid line indicates that the Army DF is primarily covered by the USFCDF. Note, in some cases, the USFCDF is broad enough to cover more than one USFCDF. The dotted arrow indicates partial coverage by the corresponding USFCDF. In some cases, the Army DF is covered by more than one USFCDF. No single USFCDF provides full coverage. Note that one Army DF (#16 Alignment)and one USFCDF DF (R1 Security)

do not have a corresponding arrow linking them. These orphan DFs are discussed later in this section.

After mapping the Army DFs to the USFCDF DFs, the next step toward answering this first research sub-question is to apply set theory and determine whether the mapping of set of Army DFs to USFCDF DFs was surjective (also referred to as onto). USFCDF DFs are surjective if every element of the USFCDF is mapped to by at least one element of the Army set of DFs. The mapping of the Army DF's to the USFCDF was not fully surjective at the time the Army made their critical decision for Cloud because none of the Army DF's used at the time of the decision mapped significantly to the USFCDF DF R1 – security requirements.

It would appear implausible that the Army would not include security as a DF. Security has been identified through surveys and at conferences on the Cloud topic to be one of the top concerns of Federal IT decision makers. For example, Cloud security was the sole topic of a one-day government-industry session by the IT leader responsible for security at the largest IT organization in DoD (Mink 2010).

It turns out that the Army considered security a very important DF. This can been seen in the Army's initial set of DFs (see Figure 34), when security was included.(Army 2008) The Army considered security so important that the they made it a threshold requirement – any option for Cloud must prove secure before being considered for a formal decision. The threshold aspect of the Army security DF was summarized by LTC Barclay during the case research, "Because if we had something that was at risk of being secure it wouldn't be a course of action. That gets strained out to start with." When asked to rank

the USFCDF DFs, LTC Barclay ranked Security highest among all the USFCDF readiness DFs.

The importance of security as a DF was further emphasized by LTG Sorrenson during his interview. He too ranked security requirements as number one in importance. Therefore, with security implicit as a threshold, or prerequisite – and all other USFCDF DFs covered by other Army DFs from the mapping in Figure 33, the set theory analysis finds that all USFCDF DFs were necessary for the Army decision to migrate to Cloud.

This finding can be further validated by checking whether the lowest ranking USFCDFs were still considered necessary by those interviewed for this case. The interviewees were asked to rank the USFCDF DFs, and then asked whether any of the USFCDF DFs would not be of value (i.e. unnecessary) for their Cloud migration decision. Table 15 summarizes the rankings given the USFCDF DFs by those interviewed during the case study.

Table 15 - Army Ranking of USFCDF Decision Factors

USFCDF DECISION FACTORS		ARMY		
		Sorrenson	Barclay	AVG
VALUE FACTORS				
V1	Efficiency	1	1	1
V2	Agility	2	2	2
V3	Innovation	3	3	3
READINESS FACTORS				
R1	Security	1	1	1
R2	Service Characteristics	3	2	2.5
R3	Market Characteristics	6	3	4.5
R4	Network, App & Data Readiness	2	4.5	3.25
R5	Government Readiness	4	4.5	4.25
R6	Technology Lifecycle	5	6	5.5

The lowest ranking DF in the value category was innovation. Both interviewees rated it last. If any of the three value DFs were unnecessary, based on the expertise of the two key stakeholders in the Army's Cloud migration decision, then it would have been the innovation DF. Yet, despite its low ranking, the innovation DF was important to the Army's decision. Innovation directly mapped to what the Army sought for Flexibility. Furthermore, the Army's concern for their acquisition strategy and their integration with Active Directory both mapped to the USFCDF innovation provided by Cloud.

A similar analysis of the lowest ranking (least important) USFCDF readiness DF – technology lifecycle – indicated the Army considered this DF necessary as well. The Army was hosting email at each post, camp, and station. They used Microsoft Exchange 2003 which was obsolete. They knew they needed to upgrade to Exchange 2007 or the upcoming Exchange 2010 (Barclay 2012). LTC Barlclay also indicated that such an upgrade to the software would drive a requirement to upgrade from 32-bit to 64-bit servers. Finally, the legacy system needed significant investment to incorporate better security through the Common Access Card as well as better interoperability through restructuring and consolidating the Army's Active Directory. They clearly considered the lifecycle stage of their legacy IT system – and therefore the USFCDF technology lifecycle DF -- a necessary factor in their decision to migrate to Cloud.

As an additional investigation to determine whether all USFCDF DFs were necessary, each interviewer was asked whether any of the nine USFCDF DFs was unnecessary. Both interviewees indicated that all USFCDF DFs were useful for a Cloud migration decision.

Given the finding that all the USFCDF DFs were necessary, the next sub-question considers whether the USFCDF lacked any DFs needed by the Army.

Q1b - Is the set of USFCDF decision factors sufficient?

This sub-question asks whether any DFs needed by the Army were missing from the USFCDF set of DFs. The set of USFCDF DFs would be found sufficient if together they incorporated all the factors considered by the Army. As noted earlier, the Army used a different set of DFs from the USFCDF. The same mapping in Figure 33 that was used to answer Q1a can also be applied to help answer Q1b. Again, set theory is applied, but this time analyzing the mapping coverage of the Army DFs – determining whether any Army DF lacks a mapping to a corresponding USFCDF DF.

As seen in Figure 33, sixteen of the Army's seventeen DFs were covered by one or more of the USFCDF DFs. These sixteen are: Acquisition Strategy, Flexibility, Agility, Speed, Adaptability, Integration with AD Plan, Scalability, Org Change Management, Migration – In, Migration – Out., Sustainment Costs, Initial Investment, Transition costs, Operational & Technical Risk, Cooperation, and Schedule. The remaining Army DF (Alignment – Resources with Implementation) was not covered by a USFCDF DF and therefore merits further analysis.

The Army defined this remaining DF (referred to as alignment in this section) as "Risk the funding stream will not support the COA implementation plan." This DF differs from the three financial DFs mapped to the USFCDF efficiency DF – sustainment costs, initial investment, and transition costs. These three Army financial DFs relate to the cost-

benefit analysis of the Army business case for Cloud and therefore clearly map to USFCDF efficiency DF. On the other hand, the Army alignment DF relates to the Federal budgeting and acquisition regulations. Funds for projects are requested, appropriated, and spent in accordance with guidance from Congress, the Office of Management and Budget, and other stakeholders in DoD resourcing. Unlike commercial firms, Federal Agencies face restrictions that limit their ability to move funds from one project to another, and from one type of funding to another – for example from sustainment to procurement.(USD(AT&L) 2008). This set of funding restrictions is often referred to as the "color of money." Budget officials strive to ensure that the correct color of money is used for an expense. Further complicating IT initiatives such as Cloud migration, Federal Agencies are often under a spotlight by Congress, GAO and others. This emphasis on oversight can be justified by the amount of taxpayer funds involved, but often external stakeholders – perhaps firms whose solution was not adopted by the Federal Agency – will devote their own resources to inform stakeholders about problems with Federal IT projects. For example, in October 2010, Google and its licensed vendor Onix Networks filed a pre-award complaint in the United States Court of Federal Cl against the US Department of Interior (DoI) because DoI was embarking on an IT procurement limited to Microsoft Exchange, which precluded Google's email solution (Courts 2011).

One can surmise why the USFCDF omitted a consideration for how a Cloud migration might be affected by Federal Acquisition Regulations (FARs). Kundra, who spearheaded the UDFCDF had a commercial and academic background – and not Federal Government

experience. Furthermore, senior leaders understand that some regulations can be changed, and perhaps they felt that regulations restricting Cloud migration would be modified.

However, regardless of the reason why the USFCDF lacks a DF to cover the Army's alignment DF, it does not appear that its absence is significant. The Army ranked the alignment DF low on the Army COA rankings (Barclay 2012). Furthermore, the Army decision maker did not consider components of the alignment DF -- such as the color of money discussed earlier -- significant for his decision (Sorenson 2012). While this case finds that there may be a small benefit in including the Army alignment DF into the USFCDF – or modifying an existing USFCDF DF's scope to include alignment -- the omission of this DF does not appear to be a significant shortcoming of the USFCDF. The finding of the second sub-question is that yes, the USFCDFs were generally sufficient for the Army migration decision.

Q2. Does the USFCDF decision structure provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

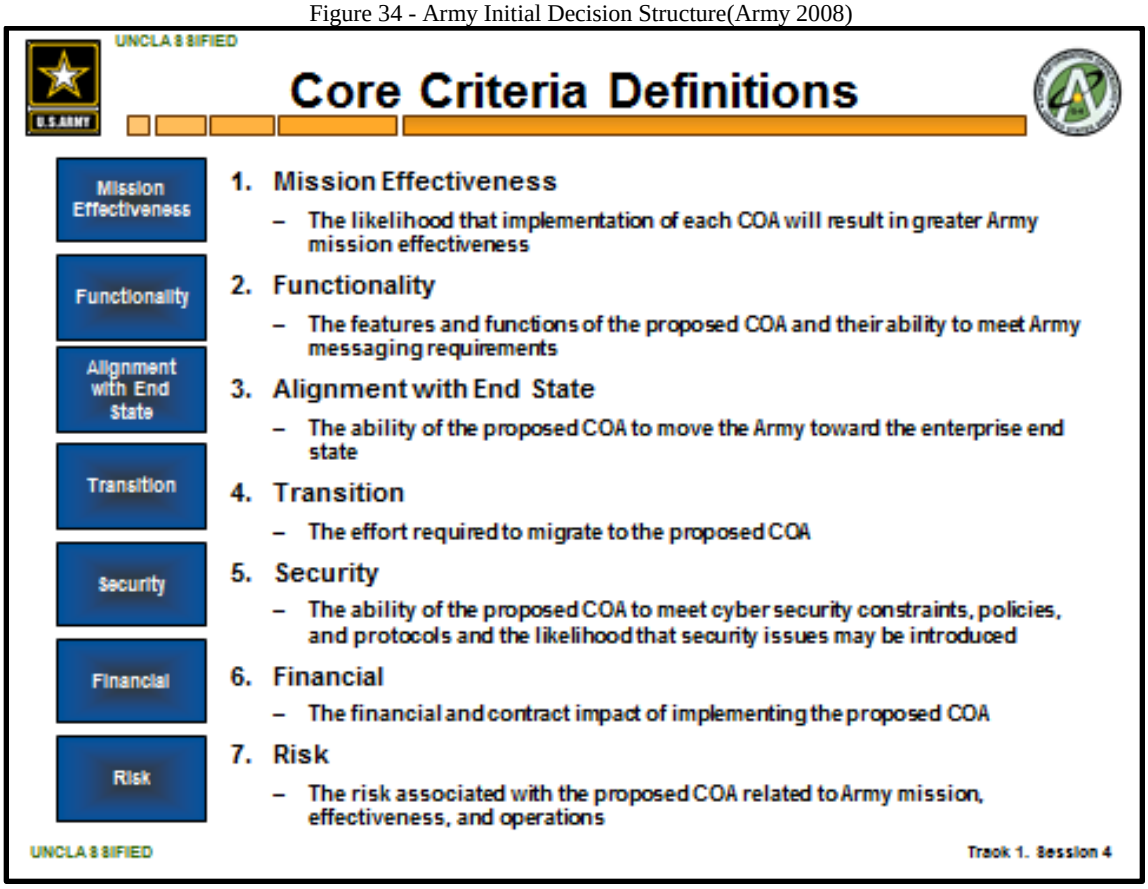
The second research question involves the USFCDF decision structure (DS). A decision structure – such as the USFCDF DS or others – is simply a construct to organize individual DFs into categories or buckets of DFs, which provides decision makers a higher-level understanding of the elements of the decision. The first sub-question relates to DS's in general, and not specifically to just the USFCDF DF.

Q2a - Does a decision structure (in general) provide value?

To answer this sub-question, the researcher analyzed the Army Cloud migration decision to determine whether the Army applied a decision structure to marshal their DFs.

The Army first developed a DS in 2008 as part of their preparation for the Cloud migration decision. Their initial DS consisted of seven categories they termed "Core Criteria."(Army 2008) These original Army DS categories, along with the definitions for each DS category, are listed in Figure 34.

Figure 34 - Army Initial Decision Structure(Army 2008)



These seven core criteria which formed the initial DS in 2008 evolved to the five-dimensional DS applied in 2010 for the actual Cloud migration decision. Table 16 depicts the five categories of the final 2010 Army DS.

Table 16 - Dimensions of Army Decision Structure(Barclay 2012)

Strategy Effectiveness
Alignment with End-State
Transition
Financial
Risk/Feasibility

The Army found value in focusing their DFs through a DS that enabled them to depict a complex set of factors through a simpler categorization. Furthermore, the Army used this DS to create high-level weightings across the five DS categories, which then put the weightings of the individual DFs into a larger perspective(Barclay 2012). The finding from researching sub-question 2a is that a DS provides value to the Cloud migration decision maker.

Given the value of a DS in general for a Cloud migration decision, the next sub-question asks whether the USFCDF DS is of use as a basis for a Cloud migration DS.

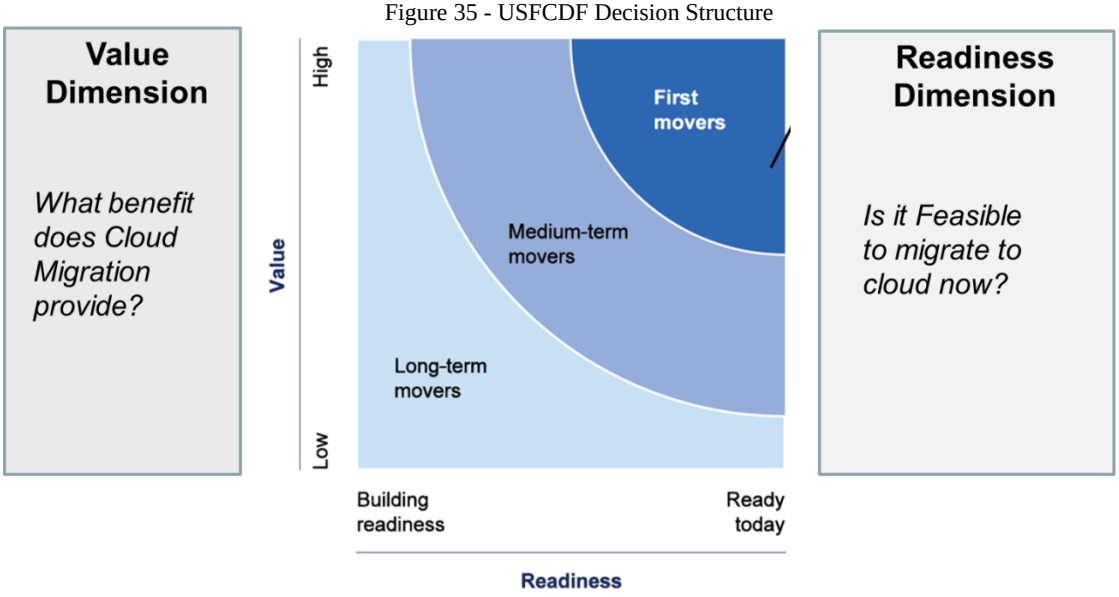
Q2b - Is the Value-Readiness paradigm of the USFCDF decision structure useful for marshalling decision factors?

The originator of the USFCDF declared that, "the logic and structure of the framework should be applicable for all agencies."(Kundra 2011). The Army evolved their DS independent of the USFCDF DS. The Army also invested considerable effort to craft and evolve their DS – leveraging experts and hiring Gartner as consultants. Finally, the Army felt their DS was appropriate and useful for their eventual Cloud migration decision. Therefore, should the USFCDF DS be found to be similar to the Army DS, it follows that Kundra's declaration was valid and the USCDF DS would be useful for marshalling DFs for Cloud migration decisions.

To answer this sub-question, this investigation first researched the two dimensions of the USFCDF decision structure, comparing them to the elements of the leading model for technology acceptance. Armed with insights from that first step, the investigation then compared the USFCDF DS with the Army DS to identify similarities and differences.

For the first research step described above, the researcher compared the USFCDF DS to the Technology Acceptance Model (TAM). The USFCDF DS was described fully in Chapter 2. The USFCDF DS consists of two dimensions: value and readiness. These are depicted in Figure 35.

Figure 35 - USFCDF Decision Structure



According to the Federal Cloud Computing Strategy, the value dimension captures the benefits of Cloud migration while the readiness dimension "broadly captures the ability for the IT service to move to the cloud in the near-term."(Kundra 2011)

These two dimensions of the USFCDF DS align closely with the two variables of the TAM. TAM is arguably the most validated model for predicting user adoption of new technologies(Davis 1989). TAM suggests the two variables for predicting user adoption

are perceived usefulness and perceived ease of use. As seen in Table 17, the USFCDF and the TAM align rather closely – both using two dimensions with similar dimensions.

Table 17 - Comparison of USFCDF Decision Structure to Technology Acceptance Model[6]

	USFCDF		TAM	
1	**Value**	Captures benefits	**Usefulness**	A system will enhance job performance
2	**Readiness**	Captures the ability for the IT service to move to the cloud in the near-term.	**Ease of use**	Using the system would be free of effort

For the first dimension (row 1 in the table above), USFCDF considers value to be what the Federal Agency gains by migrating to Cloud. TAM considers the usefulness of the new system for those using it. Arguably, USFCDF value and TAM usefulness suggest similar considerations, but from differing perspectives. For the second dimension (row 2in the table above), USFCDF considers readiness for Cloud migration while TAM considers how easy a user will find the system to use. When one understand that the USFCDF readiness dimension considers how easy a Federal Agency will find a migration to implement, it suggests again that the USFCDF DS and the TAM are parallel constructs.

The close alignment of the two dimensions of the USFCDF with those of TAM suggests that other useful Cloud migration DS's should also align with the USFCDF value-readiness paradigm. For this case, the research investigated the alignment of the USFCDF with the Army DS.

[6] Definitions relate to the Federal IT decision maker for USFCDF and a user for TAM. In both frameworks, the evaluation assumes some level of subjective individual perception.

The Army formulated its original DS in 2008 and then evolved it to final DS used in 2010. Based on that timetable, the Army had to have developed its DS prior to the USFCDF being published. From all investigations, the Army was unaware of the USFCDF effort and was not influenced by the USFCDF. In other words, the Army DS and the USFCDF DS were developed independently.

The Army DS, although developed independently from the USFCDF, also aligns significantly with the USFCDF, suggesting the USFCDF could be of value as a Federal Agency begins to frame. This alignment can be seen by comparing the definitions of the DS's dimensions and then by analyzing the mapping of the Army decision factors onto the USFCDF DFs – to analyze whether the DFs belonging to a particular Army DS category correlate to the dimensions containing the corresponding USFCDF DFs.

The Army DS consists of five dimensions listed in Table 16. Comparing the Army DS definitions to those of the USFCDF, the following can be observed:

1. The Army decision structure was similar to the USFCDF in that a major decision category for the Army was feasibility/risk, which roughly paralleled the USFCDF's readiness category.
2. To provide greater visibility and weight for the challenges of the Cloud transition itself, the Army broke out those decision factors related to transition into a separate DS category labeled Transition. Success in the transition to Cloud (prior to the Cloud reaching full operational capability) to Cloud clearly depends on the readiness of all the stakeholders to implement Cloud-based email. The

observation is that the Army transition category too maps to the USFCDF readiness dimension.

3. The third Army DS category is financial. Financial's definition as a DS category is nearly identical to the USFCDF's DF definition of its efficiency DF. In this case though, Army elevated their financial considerations to a DS category, while efficiency remains a lower DF. There is simply is a difference in priority/hierarch. The Army financial category is covered by the efficiency DF within the USFCDF DS value dimension.
4. The remaining two Army DS categories area: a) strategy effectiveness and b) alignment with (Army) end state. Both of these convey the benefits of Cloud – including agility and innovation, and therefore arguably align with the USFCDF DS dimension of value.

Based on definitions, the categories of the Army DS align are consistent with the value-readiness paradigm of the USDFCDF DS.

An analysis of the Army DF mapping to the USFCDF DFs should indicate a similar alignment. Should the DFs belonging to an Army DS category map primarily to the DFs contained in a given dimension of a USFCDF, then it would suggest that the Army DS category and the USFCDF dimension were aligned as well. Table 18 depicts the alignment of the Army DFs associated with each Army DS categories with the USFCDF DFs associated with each UFCDF dimension. The correlation factors in the table indicate the ration of the mapping of the DFs for a given Army DS category to the corresponding USFCDF dimension. A neutral correlation, or balanced would be indicated by .5 – with

half of the Army DFs in the category mapping to the USFCDF value dimension and the other half mapping to the USFCDF readiness dimension. On the other hand, a perfect correlation would be indicated by 1.0 – with all the DFs for that Army DS category mapping to (only) one of the two USFCDF DSs.

As can be seen from Table 18, the results of the correlation of the DFs match the earlier results analyzing the definitions of the two decision structures.

Table 18 - Alignment of Case DS to USFCDF DS (Based on Correlation of DFs)

	Alignment with USFCDF Dimensions[7]	
Army DS Category	**USFCDF - Value**	**USFCDF - Readiness**
Strategy Effectiveness	0.75	0.25
Alignment with End-State	0.67	0.33
Transition	0.00	1.00
Financial	0.83	0.17
Risk/Feasibility	0.00	1.00

Not only does Table 18 indicate an alignment between the Army DS and the USFCDF DS, but the alignment is exactly the same as predicted by the analysis of the definition of the two DS's.

The answer to sub-question 2b is that a Federal IT leader would receive value in preparing for a cloud migration by adopting the USFCDF value-readiness paradigm as a starting basis for their decision structure. This is supported by alignment of USFCDF DS to the Technology Acceptance Model as well as the alignment of the USFCDF DS

[7] Ratio of DFs in the case study to DFs of the USFCDF. See Figure 33 for a depiction of the DF mappings.

dimensions to the Army DS categories. A Federal IT leader would benefit by either using the USFCDF DS as is, or by starting with it as a baseline and modifying it to elevate or highlight certain sub-elements of either value or readiness.

Q3. Does the USFCDF decision question provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The third research question is about the decision question (DQ). The DQ represents what it is that the decision maker should answer as the basis of his/her decision. In USFCDF, the general problem is to "Identify which IT services to move and when."(Kundra 2011) This implies that the DQ for a specific legacy IT system is to ask "should this legacy system migrate to the Cloud, and if so, when?" The USFCDF DQ can be seen in two parts, the primary part about appears as a binary decision – migrate or do not migrate. The secondary part considers the timing of the migration.

This primary part of the DQ is consistent with prior works (mostly surveys) that investigate the considerations for deciding whether a system should migrate to the Cloud or not. This case study research investigates whether the USFCDF DQ is consistent with the type of DQ needed to make Cloud migration decisions in the Federal Government. The research consists of two sub-questions, one relating to regulations from the Federal Government in general, the other related to the Army's approach to their DQ.

Q3a. Is the USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions?

Unlike commercial firms, Federal Agencies are bound by a complex set of regulatory guidance describing – often in significant detail – what is required of a Federal IT leader for decisions related to IT purchased by Federal funds. Therefore, Cloud migration decisions need to comply with this regulatory guidance.

The foundational regulation that covers Cloud migration is the Federal Acquisition Regulation (FAR) and for DoD, the Defense Federal Acquisition Regulation Supplement (DRARS). They require the Federal IT leader to shape their decision as a selection among alternatives: "Discuss feasible acquisition alternatives, the impact of prior acquisitions on those alternatives, and any related in-house effort."(GAO 2005)

At first, this might suggest that the USFCDF DQ – as a binary question to migrate or not migrate – might be inconsistent with the FAR However, by casting the decision as a choice among two alternatives -- the status quo (legacy IT system) and a cloud migration – the Federal IT leader can adopt the USFCDF DQ while remaining consistent with the FAR. Furthermore, this approach explicitly incorporates other FAR guidance. For example, by explicitly listing the status quo (legacy IT system) as an alternative, the Federal IT leader explicitly relates the impact of the legacy system to the Cloud migration alternative. This applies whether that legacy IT system was initially acquired or developed in-house.

The finding for sub-question 3a is that USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions.

Q3b. Is the USFCDF decision question consistent with the needs of the decision maker

The Army complied with FAR by casting the Cloud migration DQ as an analysis of alternatives. Their DQ include the status quo – the legacy Microsoft Exchange email system hosted at nearly every significant Army installation. But, instead of listing Cloud migration as the single alternative to the status quo, the Army identified three alternatives to the status quo. The Army referred to these alternatives as "Courses of Action (COAs)" a term often applied to alternatives evaluated by a commander for a military combat decision. The Army's DQ – depicted as COAs – is summarized in Table 19.

Table 19 - Army Decision Question, Depicted as COA's[8]

Course of Action	Description	- Owner - Operator	Cloud? - Deployment Model - Delivery Model
1 Status Quo	Use existing [legacy Microsoft] Exchange 2003 (with planned technology refreshes)	- Army - Army	Cloud? No
2 Commercial MSP	Purchase email service from a commercial Managed Service Provider (MSP).	- Contractor - Contractor	Cloud? Yes - Private - SaaS
3 Army Knowledge Online	Upgrade existing AKO capability to meet requirements	- Army - Contractor	Cloud? Somewhat - Private - SaaS
4 DISA MSP	Acquire Enterprise Email as a service from the Defense Information Systems Agency (DISA)	- DISA - DISA	Cloud? Yes - Community - SaaS

[8] This table was compiled from multiple sources, including: Army's Initial Draft of Analysis of Alternatives, Interview with LTC Barclay, and the 2012 Army Report to Congress on Enterprise Email. (Army 2012)

Although the Army's Cloud migration decision was shaped independently of the USFCDF, the result was an extension of the USFCDF binary yes-or-no decision to an AOA with the status quo mapping to the USFCDF "no" alternative and multiple Cloud (and partial Cloud) alternatives mapping to the USFCDF "yes" alternative. This approach enabled the Army to be compliant with FARs[9] while also considering competing Cloud solutions for their Cloud migration.

The answer to question 3b is that the USFCDF DQ is consistent with the needs of the Federal IT decision maker – by extending the binary yes-or-no USFCDF DQ to an analysis of alternatives that includes the status quo.

Q4. Is email a well-defined legacy IT system?

The fourth research question inquires about whether email represents a well-defined legacy system across the Federal Government. A well-defined system is indicated when its functionality and system quality attributes are well known and documents – and often implemented by competing IT vendors. This is in contrast to unique, proprietary systems that would require a Federal Agency to capture a list of functional requirements and system quality attributes. Furthermore, a legacy system that is not well defined is not likely to have competing vendors providing similar capabilities that would be exchangeable with the legacy system. If email is found to be a well-defined legacy system, then it can be argued that the results of this research project could be generalized to other well-defined legacy IT systems across the Federal Government.

[9] By selecting email from DISA, technically Army was relieved of some of the requirements of FARs. But, because commercial providers were under consideration – and originally were thought of as the likely outcome of the Cloud migration decision, the Army wisely adopted a FAR-compliant DQ.

This case researched two sub-questions, one questioning whether the Army's legacy email system (the status quo) was well-defined, and the other about whether email was widespread across the Army such at this represented an Agency –wide legacy system.

4a. Are email systems in the Federal Government defined by a small set of similar legacy commercial products?

The Army defined its email requirements based on the functionality provided by its legacy email system – Microsoft Exchange 2003. Any replacement – Cloud or otherwise – was expected to deliver the capabilities equivalent to the next version of Microsoft Exchange(Olson 2009). Furthermore, the primary user interface for email in the Army was a desktop client, Microsoft Outlook. By requiring interoperability – and full support for its functionality – any replacement for the legacy system was very well defined. That the Army eliminated DFs related to the "functionality" between their initial exploration in 2008 and their final decision in 2010 indicates how well-defined Army considered their legacy email system(Army 2008). The answer to question 4a is that the Army had only one primary legacy system – Microsoft Exchange – and considered it well-defined.

4b. Is email used across the Federal enterprise?

This case study only researched the Army. However, the Army is the largest Service in the DoD, with 1.4 million users. Furthermore, by selecting DISA as their Cloud solution for email, DISA was in a position to provide email to other DoD organizations by employing the NIST-defined community Cloud deployment model. Subsequent to the Army's decision to select DISA as their email Cloud provider, the DoD Chief Information Officer tasked all DoD Components to develop an implementation plan that will "initiate migration to DEE [Defense Enterprise Email] no later than 1st Quarter of

Fiscal Year 2015(Takai 2013). With DoD as the largest Federal Agency, this implies that not only is email used across the largest Federal Agency, but that the Army's Cloud migration decision proved sufficient to abrogate the need for other DoD organizations to make such a decision – the decision was made for them by the DoD CIO.

Q5. Would Cloud migration decision-makers have benefited from prior-knowledge of a validated USFCDF?

The Army suffered from being a first-mover in DoD for a Cloud migration because it had to break new ground and defend itself throughout the process. Unfortunately, the Army compounded this challenge not formally documenting their Cloud migration decision – the final decision documents were not signed when the decision was made.(Barclay 2012). After their decision, the Army was questioned about their decision and required to defend their decision. For example, Congress, in Section 353 of the National Defense Authorization Act for Fiscal Year 2012, limited funding for the Army's cloud-based enterprise email until the Army answered questions about the decision to migrate legacy email to the Cloud. Congress directed the Army to provide:

- "An assessment by the acquisition oversight body of the sufficiency and completeness of the current validated requirements and analysis of alternatives.
- In any instances where the validated requirements or analysis of alternatives has been determined to be insufficient, a plan for remediation." (Burrelli 2012)

Note that both bullets question the analysis of alternatives, implying Congress lacked confidence in the Army's decision framework (consisting of the Army DFs, DS, and DQ).

Clearly, the Army's defense of their decision would have been enhanced had they been able to trace their decision framework to a pre-validated decision framework such as the USFCDF. This finding is further supported by the interviews of the Army Cloud migration action officer who led the decision analysis leading to the decision as well as the Federal IT leader who made the Cloud migration decision. When asked if, at the start of the decision process (prior to April 2010 in this case) the Army had a decision construct that was objective, validated, and contained an initial set of decision factors – would that have been beneficial? LTC Barclay stated "I think it would have been great value…" LTG Sorrenson summarized this by asserting "Oh, absolutely. Without question." He went on to indicate "There were a lot of things that we didn't know what we didn't know as we were trying to make sense of how to move forward here," implying that a framework such as the USFCDF would not only be useful to defend a Cloud migration decision after the fact, but also to accelerate the preparation and result in a better up-front analysis to prepare for the Cloud migration decision.

Other Findings and Observations

In addition to findings directly related to the five research questions and their sub-questions, this investigation identified other observations relevant to the research topic and that would be of interest to others investigating the topic of Cloud migration in the US Federal Government.

Army 01 - The decisions process and associated decision gates

The decision process proceed through a series of gates that started prior to the primary Cloud migration decision and extended into the start of the cloud migration itself. For

example, the Army originally considered a commercial Cloud provider for a private email cloud, but the timing of funds available caused them to reconsider and include DISA as a COA for their DQ. As noted earlier in this case study summary, the Army originally included security as a category of their Cloud decision structure but later removed security from the final Cloud migration decision. Between decision gates, they decided that security was foundational, and that any course of action evaluated would be first assessed for adequate security prior to the formal Cloud migration decision.

As a result of the multiple decision gates, the Cloud decision itself was revisited over time, causing the DFs, DS, and DQ to evolve as well as the outcome of the decision itself. Given the multiple gates over time, the researcher adopted the decision that led to Cloud migration that was actually implemented for the findings and observations in this case study summary. This also suggests that in the future, the Army and other Federal Agencies will likely encounter a series of decision gates prior to the final decision that results in the actual migration to Cloud.

Army O2 – Decision documentation

The absence of formal documentation about the early decision gates – and even from the decision that led to the implemented cloud migration -- adversely affected the subsequent implementation of the Army cloud migration. This observation supports the value of having a common Federal decision framework – to act as a template to collect the decision data prior to the decision, and to serve as the details for the formal decision memo itself. Not only did the circumstances of the case make this obvious, but the decision maker himself made the same observation during the case interviews.

Army O3 – Cost and efficiency

The Army ranked cost savings high in their decision preparation. Efficiency also ranked high by those interviewed for the case study. And, the Army report to Congress forecast a savings of $379.9M over five years. Yet, it would appear that a significant portion of those savings results from standing down Army Knowledge Online, which had provided lifetime email and a second email account for Army. Furthermore, the savings forecast had eroded over time. In its report to Congress on its Cloud migration, the Army Audit Agency concluded "the savings claimed (originally more than $100 million per year), though still significant, were overstated." Evidence from the case study research documents indicates that the Army's estimated five-year savings dropped by $206M between their analysis in September 2010 and their analysis in February 2012.

Army O4 –Federal guidance and Cloud migration

Around the time of the Army decision to migrate their email to the Cloud the Federal CIO, Vivek Kundra, released guidance for Federal Agencies to adopt Cloud, "When evaluating options for new IT deployments, OMB [US Office of Management & Budget] will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists."(Kundra 2010) Although Kundra released this guidance a month after the Army Cloud migration decision, Army IT leaders were aware of Kundra's initiative. Both LTG Sorrenson and LTC Barclay indicated that they felt such guidance created additional weight for migrating to Cloud. In a larger sense, migrating to Cloud has also become a matter of compliance with another piece of Federal regulation. This indicates a potential research project to study whether "compliance" with Federal mandates should be incorporated in the USFCDF.

Army O5 – Acceptance of NIST Cloud definitions

At the time of this research project, Federal Agencies lacked a clear, common definition of Cloud, the characteristics of Cloud, how Cloud service models are categorized, and how Cloud deployment models are defined. This research project adopted the early draft by the National Institute of Standards and Technology (NIST). This approach was validated by the Army, which had also adopted the emerging NIST definitions for Cloud for their Cloud migration decision process.(Olson 2009)

Summary & Conclusions (Case 1 – Army Enterprise Email)

The Army's cloud migration decision predated Kundra's decision framework and decision factors so the Army's decision framework was not influenced by the USFCDF. Independently, the Army developed a decision framework that supports the value of the USFCDF. All the USFCDF DFs were necessary. The set of USFCDF DFs was generally sufficient, but may benefit by incorporating what the Army termed "alignment of resources with implementation." The USFCDF DS, with its value-readiness paradigm is consistent with other models related to technology adoption, and aligns with the Army's DS. The USFCDF DQ, a basic yes-or-no question, was extended by the Army to conform to acquisition regulations and allow the decision maker to choose from several Cloud alternatives. This case found support for extending the findings for email to other well-defined legacy IT systems. Finally, this case suggests IT leaders will value a decision framework such as the USFCDF.

Case 2 – National Science Foundation (NSF) Email

This case study summary provides the findings and observations surrounding the August 2010 decision by the National Science Foundation to migrate their legacy email systems to cloud. The senior decision-maker, Dorothy Aronson, Special Assistant to the Director for IT Operations, led the decision making process. Her team selected Software as a Service (SaaS) for their cloud delivery model (see Chapter 2). The specific Cloud vendor solution was withheld from this report at the request of the NSF because the vendor was not yet under contract.

The investigations for this case followed the methodology described in Chapter 3. NSF's champion for this research investigation was the NSF CIO, Amy Northcutt. Investigative sources for the case included Amy Northcutt as well as Nick Ipiotis, Infrastructure Service Branch Chief, and a third senior IT leader who requested anonymity (subsequently referred to as Interviewee three or I3). Some NSF documentation – particularly working papers surrounding the decision also informed this case study investigation.

The next sections summarize the findings and observations from this case study. See the appendices for more background and context on this case.

Q1 - Do the USFCDF decision factors provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The NSF formally established a five-category decision structure as depicted in Figure 36, but the DFs in each category were less-well defined. The DFs discussed in this chapter

consist of the researcher's breakout of pieces of the explanation that accompanied each of the DS categories. Much like parsing a sentence, each NDF DS category description used by the NSF was parsed to identify a set of DFs for that category.

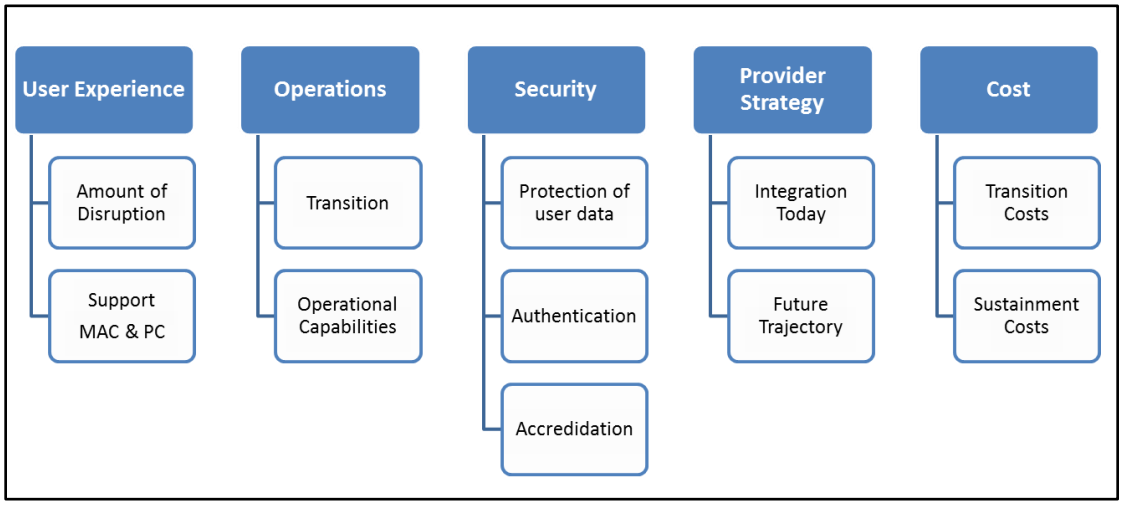


Figure 36 - Eleven NSF Decision Factors: Organized by Six Decision Structure Categories (Ipiotis 2012) [10]

These eleven NSF DFs are defined in Table 20.

[10] The DFs were not identified by NSF as explicit factors individually weighted. Instead, these DFs represent the key components extracted from the description of each DS category.

Table 20 - NSF Decision Factors: Definitions (Ipiotis 2012)

#	Decision Factor	Definition
1	Amount of disruption to user	Limited downtime for user. Little change apparent to user.
2	Support for MAC & PC	Ability to support users with Apple MACs using the MAC email client as well as with PCs using the Microsoft email client
3	Transition	Migration of email data from the legacy system to the new capability as well as interfacing or integrating key NSF systems that are interdependent on the email capability
4	Ongoing Operations	Administrative activities like account management, document management (e.g. Freedom of Information requests), and purging select emails.
5	Protection of User Data	Ensuring the protection of user emails and attached documents
6	Authentication	Validating a user and providing the user access to data based on the user's location.
7	Accreditation	The new email capability has been accredited for security
8	Integration Today	The vendor's position, strategy, and stability to integrate with NSFs other systems
9	Future Trajectory	Commitment to continue enhancing the service
10	Transition Costs	Financial costs for migrating to the new Cloud capability
11	Operating Costs	Financial costs for operating the service once the capability was in operation.

To answer question 1, the researchers compared the eleven DFs used by the NSF (see NSF DF definitions above) to the nine USFCEF DFs described in Chapter 2 (listed on the right side Figure 37). This comparison, along with other supporting evidence, was used to determine whether the USFCDF DFs were necessary and sufficient for a Cloud migration decision.

Q1a - Were all of USFCDF Decision Factors necessary for the Cloud decision?

All of the USFCDF DFs would be found necessary if the NSF applied each and every one of them in their Cloud migration decision. Because the NSF used a different set of DFs from the USFCDF, the NSF DFs were mapped to the USFCDF DFs – as depicted in Figure 37.

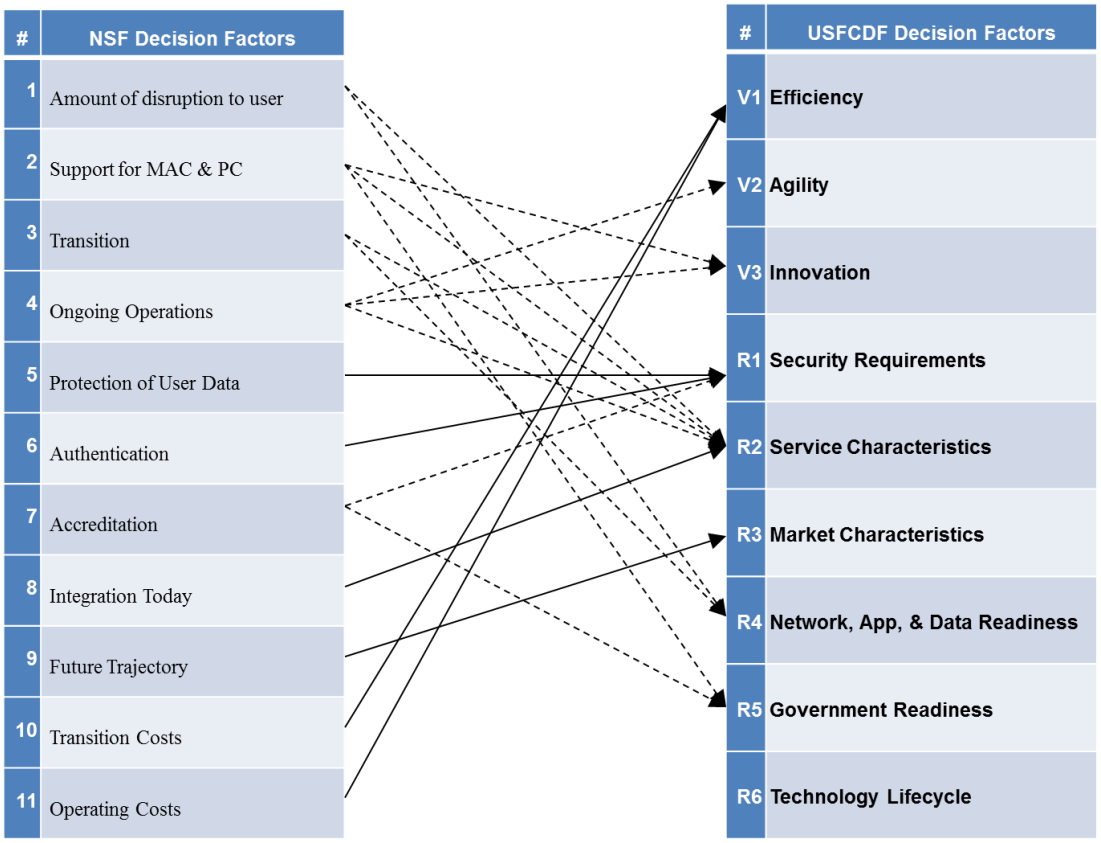


Figure 37 - NSF DFs Mapped to USFCDF DFs

Key:

NSF DF and USFCDF primarily identical

NSF DF primarily covered by USFCDF DF

NSF DF partially covered by USFCDF DF

The arrows in Figure 37 designate, for each NSF DF, the corresponding USFCDF DF(s). A double line suggests a near-identical correspondence – one to one (none for NSF). A

one-way solid line indicates that the NSF DF is primarily covered by the USFCDF. Note, in some cases, the USFCDF is broad enough to cover more than one USFCDF. The dotted arrow indicates partial coverage by the corresponding USFCDF. In some cases, the NSF DF is covered by more than one USFCDF. In that case, no single USFCDF provides full coverage for that particular NSF DF.

After mapping the NSF DFs to the USFCDF DFs, the next step toward answering this first research sub-question is to apply set theory and determine whether the mapping of set of NSF DFs to USFCDF DFs was surjective (also referred to as onto). USFCDF DFs are surjective if every element of the USFCDF is mapped to by at least one element of the NSF set of DFs. The mapping of the NSF DF's to the USFCDF was not fully surjective at the time the NSF made their critical decision for Cloud because none of the NSF DF's used at the time of the decision mapped significantly to the USFCDF DF R6 – technology lifecycle. USFCDF DF (R6 Technology Lifecycle) alone lacked a corresponding arrow mapping it from a NSF DF.

It appears that instead of NSF not considering Technology Lifecycle, this USFCDF DF was implicitly considered despite the lack of specific mention in their list of decision considerations. The USFCDF Technology lifecycle DF includes considerations for timing, to include end-of-life for legacy system components as well as anticipated future funding flows for corresponding technology refresh. The idea is that, everything else being equal, the timing for the migration to Cloud might best align to the time that the Federal Agency has to spend funds to replace obsolete legacy infrastructure. For NSF email, all interviewees noted that NSF ran Microsoft Exchange 2003, at a time when

Microsoft's current product was Exchange 2010. NSF faced a significant expense soon to upgrade Exchange. This upcoming need for technology refresh can be seen in Table 23, where NSF considers upgrading Exchange as an alternative to migrating to Cloud. This indicates that NSF considered technology lifecycle in their Cloud migration decision, but did not call it out explicitly in their decision framework.

Therefore, with technology lifecycle an implicit consideration and all other USFCDF DFs covered by other NSF DFs from the mapping in Figure 37, this set theory analysis finds that all USFCDF DFs were necessary for the NSF decision to migrate to Cloud.

This finding can be further validated by checking whether the lowest ranking USFCDFs were still considered necessary by those interviewed for this case. The interviewees were asked to rank the USFCDF DFs, and then asked whether any of the USFCDF DFs would not be of value (i.e. unnecessary) for their Cloud migration decision. Table 21summarizes the rankings given the USFCDF DFs by those interviewed during the case study.

Table 21 - NSF Ranking of USFCDF Decision Factors (By Three NSF Decision Stakeholders)

VALUE RANKINGS					
Factor	**I1**	**I2**	**I3**	**AVG**	**Statements**
Efficiency	2.5	1	1	1.5	Historically not much of a driver, but increasing 2/3rd staffing is contractors; no incentives to improve Big factor; scaling should drive efficiency We spend $100K/yr on SPAM filtering alone Important, but "assumption and hope" (no analysis done).
Agility	2.5	2.5	2	2.3	Not been a factor Faster upgrades, but help desk needs time. Exchange upgrades Ability to add/shrink number of users
Innovation	1	2.5	3	2.2	Driven by end user including MAC users. May lose functionality (a minus) Will lose some control; level of insight lost Easier to answer questions about outages
READINESS RANKINGS					
Factor	**I1**	**I2**	**I3**	**AVG**	**Statements**
Security	2.5	1	1	1.5	Dominating issue for NSF. Manage Federal data but must also be open. A threshold factor, "go / no go" Requires FedRAMP to be in place Mostly an issue with perception that cloud is less secure.
Service Characteristics	2.5	2	3	2.5	Very important. Inextricable. User experience #1 consideration FOI an example (of unique Federal needs) Blackberry and PDA an example. System reliability & availability important
Market Characteristics	4.5	4	6	4.8	Data must be easy to move. Data is ours Did not worry (about this factor)
Net App Data Readiness	4.5	5	5	4.8	App/Date secondary to security and network Important. Seamless to user.
Government Readiness	1	3	2	2.0	Adequacy & efficiency of Gov to make a decision. Good of enterprise challenged by users' feedback (Cloud) must fit the culture of NSF Must not make drastic changes (to users) IT Department fears job loss. NSF looks to GSA for security Current engineers do not now Cloud
Technology Lifecycle	6	6	4	5.3	Exchange 2003 needs to be upgraded

NSF ranked agility lowest among the three USFCDF value DFs. It tied for last place by two interviewees. If any of the three value DFs were unnecessary, based on the expertise of the two key stakeholders in the NSF's Cloud migration decision, then it would have been the agility DF. Yet, despite its low ranking, the innovation DF was important to the NSF decision. Agility directly mapped to what the NSF sought for ongoing operations. One of the IT leaders indicated that NSF, as a smaller organization, did not always have the resources to quickly install upgrades and enhancements to systems. New software releases and hardware upgrades would be on hold because they required a significant surge. Ipiotis indicated that an upgrade was considered a "project with associated labor, associated contractors to make it happen; so it was a very costly project to move versions. This was one of the huge benefits of being in a cloud system; that we can move faster." Finally, agility was mentioned as the source of NSF cost savings from Cloud in the subsequent NSF Exhibit 300 submitted to OMB. (NSF 2010-2) Therefore, it can be concluded that agility, although the lowest ranked USFCDF value DF, was still important to NSF.

And, as discussed earlier, the lowest ranked USFCDF readiness DF, technology lifecycle, was also considered necessary by the NSF for their Cloud migration decision.

As an additional investigation to determine whether all USFCDF DFs were necessary, the project lead for the Cloud migration decision was asked whether anything was missing and he responded that he felt they covered everything.(Ipiotis 2012).

Given the finding that all the USFCDF DFs were necessary, the next sub-question considers whether the USFCDF lacked any DFs needed by the NSF.

Q1b - Is the set of USFCDF decision factors sufficient?

This sub-question asks whether any DFs needed by the NSF were missing from the USFCDF set of DFs. The set of USFCDF DFs would be found sufficient if together they incorporated all the factors considered by the NSF. As noted earlier, the NSF used a different set of DFs from the USFCDF. The same mapping in Figure 37 that was used to answer Q1a can also be applied to help answer Q1b. Again, set theory is applied, but this time analyzing the mapping coverage of the NSF DFs – determining whether any NSF DF lacks a mapping to a corresponding USFCDF DF.

As seen in Figure 37, all eleven of the NSF DFs were covered by one or more of the USFCDF DFs. In other words, the existing set of nine USFCDF DFs was inclusive of the eleven NSF DFs. This conclusion was validated by queuing the project leader whether any items were missing from the USFCDF. He stated that none were missing, but he did emphasize the user experience, suggesting that the USFCDF DFs would benefit from improved wording in their definitions by finding their factors more easily in the USFCDF DF definitions (Ipiotis 2012).

The finding of the second sub-question is that yes, the USFCDFs were generally sufficient for the NSF migration decision.

Q2. Does the USFCDF decision structure provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The second research question involves the USFCDF decision structure (DS). As noted earlier, a decision structure – such as the USFCDF DS or others – is simply a construct to

organize individual DFs into categories or buckets of DFs, which provides decision makers a higher-level understanding of the elements of the decision. The first sub-question relates to DS's in general, and not specifically to just the USFCDF DF.

Q2a - Does a decision structure (in general) provide value?

To answer this sub-question, the researcher analyzed the NSF Cloud migration decision to determine whether the NSF applied a decision structure to marshal their DFs.

The NSF developed a DS as part of their decision preparation. Their initial DS consisted of five categories. The graphic in Figure 38 depicts these five categories and their relationship to each other. -

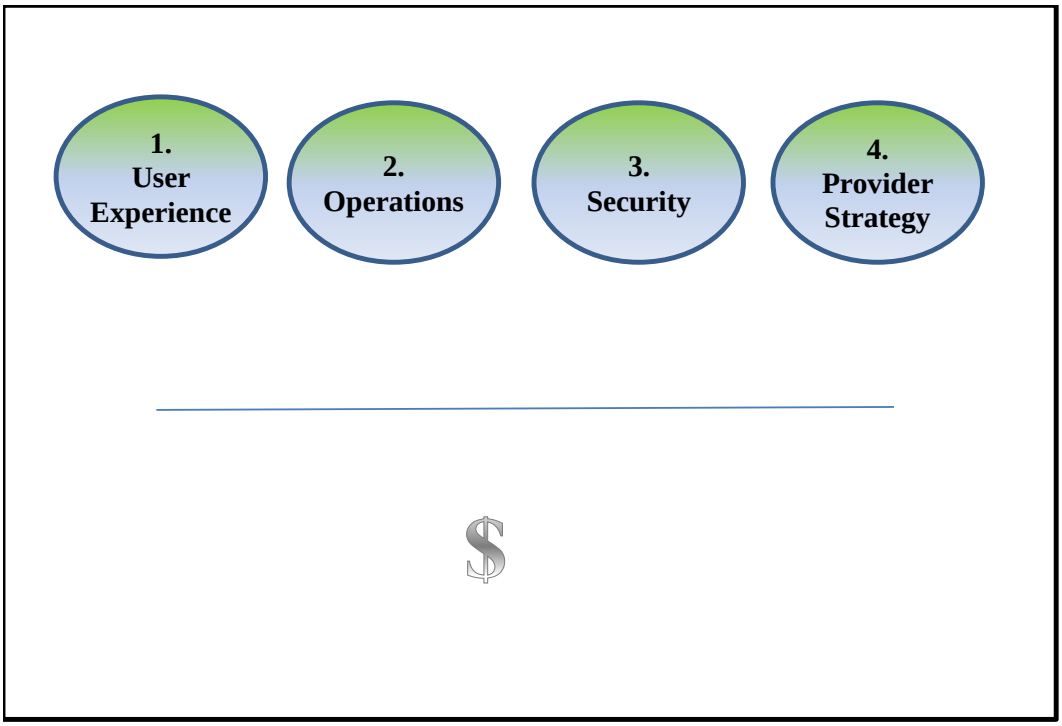


Figure 38 - Five Categories of NSF Decision Structure (Ipiotis 2012)

The NSF found value in focusing their multiple DFs through a DS that enabled them to depict a complex set of factors through a simpler categorization. Of special interest here is how NS used this DS to create a cost/benefit ratio to rate their alternatives. The top four categories were considered separately from cost; then cost was applied to normalize the result into a cost/benefit ration. The finding from researching sub-question 2a is that a DS provides value to the Cloud migration decision maker.

Given the value of a DS in general for a Cloud migration decision, the next sub-question asks whether the USFCDF DS is of use as a basis for a Cloud migration DS.

Q2b - Is the Value-Readiness paradigm of the USFCDF decision structure useful for marshalling decision factors?

The originator of the USFCDF declared that, "the logic and structure of the framework should be applicable for all agencies."(Kundra 2011). The NSF created their DS independent of the USFCDF DS. The NSF also invested considerable effort to craft and evolve their DS – leveraging feedback from its two IT governance bodies -- the Executive IT Resources Board (ITRB) and the Capital Planning and Investment Control (CPIC) Working Group. (Leader 2012) Finally, the NSF felt their DS was appropriate and useful for their eventual Cloud migration decision. Therefore, should the USFCDF DS be found to be similar to the NSF DS, it follows that Kundra's declaration was valid and the USCDF DS would be useful for marshalling DFs for Cloud migration decisions.

To answer this sub-question, this investigation first researched the two dimensions of the USFCDF decision structure, comparing them to the elements of the leading model for technology acceptance, as previously discussed in the Army case study summary.

Armed with insights from that first step, the investigation then compared the USFCDF DS with the NSF DS to identify similarities and differences. The two parts of this comparison consisted of 1) comparing the definitions of the categories from each decision framework – NSF and USFCDF, and 2) analyzing how the DFs in each NSF DS category mapped to the DFs in each USFCDF category.

The NSF DS consists of five categories depicted in **Error! Reference source not found.**. omparing these NSF DS categories to those of the USFCDF, the following can be observed:

1. The first NSF category (user experience) related to avoiding disruption and keeping the user experience similar (i.e. similar/identical user interface appearing to operate similar/identical to the legacy system). This category relates to the readiness of the Cloud offering as well as the (lack of) readiness of the users in the organization to accept changes for the greater good of the organization (lack of cultural readiness). In essence, NSF elevated aspects of two USFCDF readiness DFs to their own DS category. They align, but at different levels.
2. The second NSF category (operations) related to the effort to manage the email capability by the NSF enterprise IT organization (i.e. the NSF Division of Information Systems). NSF grouped both transition and ongoing (post transition) operations into this category. The aspect of transition is clearly related to readiness of both the service provider and the government to migrate. Transition maps to many of the readiness DFs in fact. On the other

hand, ongoing operations is concerned the value the service provides, particularly in terms of agility (incorporating patches and upgrades). Thus, it would appear that for this category (operations), the NSF applied the USFCDF DS framework against operations, looking at the value and readiness for operations. They reversed the hierarchy of the USFCDF, which considers operations a topic to be considered within value and then within readiness.

3. The third NSF DS category (security) clearly aligns with the USFCDF DS readiness dimension. The USFCDF places security as a DF, but NSF elevated security to its own DS category.
4. The fourth NSF DS category (provider strategy) captures whether the Cloud provider can integrate with the NSF today and also remain capable for NSF in the future. These relate to the service characteristics of the provider today and their position in the marketplace for the future. This maps strongly with the USFCDF DS readiness dimension.
5. The fifth NSF DS category (cost) clearly aligns with the USFCDF DS value dimension. The USFCDF places cost as a DF, but NSF elevated cost to its own DS category. Furthermore, NSF treated cost separate from the other four DSs, using it as a denominator to normalize Cloud migration decisions as a cost-benefit analysis.

Based on definitions, the categories of the NSF DS align are generally consistent with the value-readiness paradigm of the USDFCDF DS. The exceptions would be:

- NSF operations: explicitly includes readiness and value, while each of the USFCDF DS dimensions, value and readiness, explicitly include operations. The NSF DS and the USFCDF DS exhibit an inverse hierarchical relationship regarding operations.
- NSF cost: is thought of by NSF as a denominator to normalize a cost-benefit analysis, instead of being parallel to the other four NSF DS categories.

After comparing the definitions of the NSF and USFCDF DSs, the research project then analyzed the NSF DF mapping to the USFCDF DFs. A strong correlation of DFs from one NSF DS category mapping to those of a particular USFCEDF DS category should indicate DS alignment. Table 18 depicts the alignment of the NSF DFs associated with each NSF DS categories with the USFCDF DFs associated with each UFCDF dimension. The correlation factors in the table indicate the ration of the mapping of the DFs for a given NSF DS category to the corresponding USFCDF dimension. A neutral correlation, or balanced would be indicated by .5 – with half of the NSF DFs in the category mapping to the USFCDF value dimension and the other half mapping to the USFCDF readiness dimension. On the other hand, a perfect correlation would be indicated by 1.0 – with all the DFs for that NSF DS category mapping to (only) one of the two USFCDF DSs.

Table 22 - Alignment of NSF DS to USFCDF DS (Based on Correlation of DFs)

	Alignment with USFCDF Dimensions[11]	
NSF DS Category	**USFCDF - Value**	**USFCDF - Readiness**
User Experience	0.17	0.83
Operations	0.34	0.66
Security	0.00	1.00
Provider Strategy	0.00	1.00
Cost	1.00	0.00

As can be seen from Table 22, the result of the correlation of the DFs matches the earlier results analyzing the definitions of the two decision structures. The NSF operations category is fairly split, while the other NSF DS categories correlate highly with corresponding USFCDF DS dimensions.

The answer to sub-question 2b is that a Federal IT leader would receive value in preparing for a cloud migration by adopting the USFCDF value-readiness paradigm as a starting basis for their decision structure. This is supported by alignment of USFCDF DS to the Technology Acceptance Model as well as the alignment of the USFCDF DS dimensions to the NSF DS categories. A Federal IT leader would benefit by either using the USFCDF DS as is, or by starting with it as a baseline and modifying it to elevate or highlight certain sub-elements of either value or readiness.

[11] Ratio of DFs in this case study summary mapping to DFs of the USFCDF. See Figure 33 for a depiction of these DF mappings.

Q3. Does the USFCDF decision question provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The third research question is about the decision question (DQ). The DQ represents what it is that the decision maker should answer as the basis of his/her decision. This case study research investigates whether the USFCDF DQ is consistent with the type of DQ needed to make Cloud migration decisions in the Federal Government. The research consists of two sub-questions, one relating to regulations from the Federal Government in general, the other related to the NSF's approach to their DQ.

Q3a. Is the USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions?

This question was answered in the Army case study summary. Nothing in this case study summary differs from that answer. Therefore, the finding for sub-question 3a remains that USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions.

Q3b. Is the USFCDF decision question consistent with the needs of the decision maker

The NSF complied with FAR by casting the Cloud migration DQ as an analysis of alternatives. Their DQ include the status quo – the legacy Microsoft Exchange email system hosted at NSF's facility in Arlington, VA. But, instead of listing Cloud migration as the single alternative to the status quo, the NSF identified four alternatives to the status quo. The NSF referred to all five options (current NSF email and four alternatives to

status quo) as "Email Options." The NSF's DQ – depicted as email options – is summarized in Table 23.

Table 23 - NSF Decision Question, Depicted as Options (NSF 2010)

Email Option	Description	- Owner - Operator	Cloud? - Deployment Model - Delivery Model
1 Current NSF Email	Use existing [legacy Microsoft] Exchange 2003 (with planned technology refreshes)	- NSF - NSF using contractors	Cloud? No
2 Google Gmail	Purchase email service from a commercial cloud provider	- Vendor - Vendor	Cloud? Yes - Public - SaaS
3 MS Cloud "BPOS"	Microsoft's first attempt a Cloud email. Uses Exchange 2007	- Vendor - Vendor	Cloud? Mostly - Public - SaaS
4 MS Federated Cloud	Microsoft managed service offering for Exchange 2007	- Vendor - Vendor	Cloud? Slightly - Private - SaaS
5 MS Cloud "365"	Microsoft's second attempt a Cloud email. Uses Exchange 2010	- Vendor - Vendor	Cloud? Yes - Public - SaaS

Although the NSF's Cloud migration decision was shaped independently of the USFCDF, the result was an extension of the USFCDF binary yes-or-no decision to an Analysis of Alternatives (AOA) with the status quo mapping to the USFCDF "no" alternative and multiple Cloud (and partial Cloud) alternatives mapping to the USFCDF "yes" alternative. This approach enabled the NSF to be compliant with FARs while also considering competing Cloud solutions for their Cloud migration.

The answer to question 3b is that the USFCDF DQ is consistent with the needs of the Federal IT decision maker – by extending the binary yes-or-no USFCDF DQ to an analysis of alternatives that includes the status quo.

Q4. Is email a well-defined legacy IT system?

The fourth research question inquires about whether email represents a well-defined legacy system across the Federal Government. A well-defined system is indicated when its functionality and system quality attributes are well known and documents – and often implemented by competing IT vendors. This is in contrast to unique, proprietary systems that would require a Federal Agency to capture a list of functional requirements and system quality attributes. Furthermore, a legacy system that is not well defined is not likely to have competing vendors providing similar capabilities that would be exchangeable with the legacy system. If email is found to be a well-defined legacy system, then it can be argued that the results of this research project could be generalized to other well-defined legacy IT systems across the Federal Government.

This case researched two sub-questions, one questioning whether the NSF's legacy email system (the status quo) was well-defined, and the other about whether email was widespread across the NSF such at this represented an Agency –wide legacy system.

4a. Are email systems in the Federal Government defined by a small set of similar legacy commercial products?

The NSF defined its email requirements based on the functionality provided by its legacy email system – Microsoft Exchange 2003. Any replacement – Cloud or otherwise – was expected to deliver the capabilities equivalent to the next version of Microsoft Exchange (Ipiotis 2012) . Furthermore, the primary user interfaces in the NSF for email at the time

were a desktop clients: Microsoft Outlook for PCs and MacMail for the Apple Mac(Leader 2012). NSF used Exchange 2003 as the end for both user interfaces, although Exchange worked better for PCs than MACs. By requiring interoperability – and full support for the back end functionality of Exchange, as manifested by the user's ability to do email through one of two standard clients – any replacement for the legacy system was very well defined. The answer to question 4a is that the NSF had only one primary legacy system and two user interfaces, and considered their legacy system well-defined.

4b. Is email used across the Federal enterprise?

This case study indicated that email was used across the NSF enterprise of 2,500 users. (Ipiotis 2012).

Q5. Would Cloud migration decision-makers have benefited from prior-knowledge of a validated USFCDF?

The culture and past history of the NSF indicates they prefer to defer to solutions developed or validated by others before moving forward themselves. His suggests that, had it been available, they would have preferred to adopt and tailor an existing Cloud decision framework.

The earliest example is that NSF sought out others who had migrated email to the Cloud to see what they could learn and adopt from an early mover. During the interviews, the NSF IT leaders repeatedly referred to Lawrence Berkeley National Laboratory as the rationale for some of their approach to the Cloud migration decision.(Ipiotis 2012)

Another example was related to Cloud security. While some other organizations moved forward on a Cloud migration decision using their own security assessment of the Cloud

provider, NSF indicated they would defer final implementation until someone else in the US Federal Government established a security framework and assessed the Cloud provider. During the interviews, NSF indicated that they would wait for FedRAMP, the US Federal security framework described in Chapter 2, to be implemented by the Government Services Administration. (Northcutt 2012) Similarly, NSF had intended to adopt the GSA-initiated government-wide Cloud procurement contract vehicle NSF could use to obtain Cloud services from a pre-competed and evaluated Cloud service provider. (Leader 2012) NSF is also sensitive to comply with Federal guidance regarding Cloud, suggesting NSF would embrace a Federally-directed Cloud decision framework such as the USFCDF. (Leader 2012)

Although the mission of the NSF involves leading-edge research and technologies, the NSF is conservative about adopting new technologies and making changes to itself. According to the current NSF CIO, the NSF has a conservative workforce who resist change, and NSF management places a high priority on supporting the desires of that workforce. (Northcutt 2012) An externally validated Cloud decision framework would provide the NSF IT leadership with greater validity in demonstrating the value and readiness of NSF to move to Cloud. The culture and actions of the NSF related to Cloud indicate that the answer to Q5 is yes, the NSF Cloud migration decision-makers would have benefited from prior knowledge of a validated USFCDF.

Other Findings and Observations

In addition to findings directly related to the five research questions and their sub-questions, this investigation identified other observations relevant to the research topic

and that would be of interest to others investigating the topic of Cloud migration in the US Federal Government.

NSF O1 - The decisions process and associated decision gates

The decision process proceed through a series of gates that started prior to the primary Cloud migration decision and extended into a pilot of a cloud migration email option. For example, the NSF Cloud migration decision originated from a study identifying the facility requirements for NSF to move a new facility. NSF datacenter requirements would be affected by moving email out of NSF hosting and into an external hosting vendor. That decision evolved to one of exploring Cloud options in addition to just evaluating hosting options. Prior to and then after the primary NSF Cloud migration decision, NSF re-evaluated options as NSF needs evolved and vendor technologies improved. (Ipiotis 2012) This observation suggests that a USFCDF could be of value across the decision lifecycle and not just at the key Cloud migration itself.

NSF O2 – Decision documentation

The absence of formal documentation about the early decision gates – and even from the decision that led to the implemented cloud migration – was apparent at the NSF. This observation supports the value of having a common Federal decision framework – to act as a template to collect the decision data prior to the decision, and to serve as the details for the formal decision memo itself. Not only did the circumstances of the case make this obvious, but the decision maker himself made the same observation during the case interviews.

NSF O3 – Dependence on First Movers

NSF felt that progress on Cloud by other organizations was necessary before they implemented their Cloud migration. From the beginning of their decision preparation they referred to Berkley Labs and its early Cloud migration. They also stated the need for prerequisite work by other Federal Agencies. For example, NSF felt that FedRAMP, the common Federal Cloud security model for vendors, needed to be in place prior to their migration. In another example, they wanted GSA to establish a Cloud procurement vehicle to ease the burden of acquiring a Cloud vendor. NSF mentioned that their smaller size limited their resources to work these issues, and their culture caused them to be risk adverse about changes that would affect their workforce. (Leader 2012)

NSF O4 –Federal guidance and Cloud migration

Around the time of the NSF decision to migrate their email to the Cloud the Federal CIO, Vivek Kundra, released guidance for Federal Agencies to adopt Cloud, "When evaluating options for new IT deployments, OMB [US Office of Management & Budget] will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists."(Kundra 2010) Although Kundra released this guidance after NSF had prepared their decision framework, NSF leaders were aware of Kundra's initiative. All three NSF IT leaders interviewed indicated that they felt such guidance created additional weight for migrating to Cloud. In a larger sense, migrating to Cloud has also become a matter of compliance with another piece of Federal regulation. This observation indicates compliance should be considered for incorporation into the USFCDF, either through an additional DF, or by expanding the scope of an existing USFCDF DF to incorporate compliance with emerging Federal mandates.

Summary & Conclusions (Case 2 – NSF Email)

The NSF's cloud migration decision predated Kundra's decision framework and decision factors so the NSF's decision framework was not influenced by the USFCDF. Independently, the NSF developed a decision framework. The NSF decision framework suggests it aligns with the USFCDF, suggesting the USFCDF would have been beneficial to the NSF. The NSF case determined that the USFCDF DFs were necessary. The set of USFCDF DFs was generally sufficient, but may benefit by improving the definitions of some of the USFCDF DFs. The USFCDF DS, with its value-readiness paradigm is consistent with other models related to technology adoption, and aligns with four of the five NSF DS categories. For one category (operations), the NSF applied value-readiness, but subordinated value-readiness underneath the larger operations DS category. The USFCDF DQ, a basic yes-or-no question, was extended by the NSF to conform to acquisition regulations and allow the decision maker to choose from several Cloud options. This case found support for extending the findings for email to other well-defined legacy IT systems. Finally, this case suggests IT leaders will value a decision framework such as the USFCDF.

Case 3 – Veterans Affairs Cloud Email (VA)

This case study summary provides the findings and observations surrounding the May 2012 decision by Veterans Affairs to migrate their legacy email systems to cloud. The primary decision maker was Charles De Sanno, VA Executive Director of Enterprise Systems Engineering who led the decision-making process. The chief architect for the decision process was Franco Susi, Senior Systems Engineer for the VA Office of Information and Technology. A stakeholder and observer of VA's IT decisions was Ms.

Lorraine Landfried serves as Veteran Affairs' Deputy Chief Information Officer (DCIO) for Product Development (PD).

The investigations for this case followed the methodology described in Chapter 3. VA's champion for this research investigation was Roger Baker, VA CIO. Baker also served as the executive decision maker for Cloud migration and other significant IT initiatives.

The investigative sources for the case included De Sanno, Susi, and Landfried.

Some VA documentation – particularly public statements and acquisition documents about the Cloud migration also informed this case study investigation.

The next sections summarize the findings and observations from this case study. See the appendices for more background and context on this case.

Q1 - Do the USFCDF decision factors provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The VA created their set of decision factors (DFs) by considering the "pros and cons" of migrating their legacy email to the Cloud. In the words of their primary decision maker, they "backed into" these factors as they discussed the pros and cons of the migration. This resulted in the set of fifteen DFs listed in Table 24. These DFs were compiled by the researcher based on interviews, testimonies, VA's overall Cloud strategy, and a second-hand recount of the VA's internal whitepaper on email Cloud migration.

Table 24 - VA Decision Factors & Definitions

#	Decision Factor	Definition
1	Elasticity	Ability to scale capacity up and down. Growth of platform.
2	Cost	Price of initial transition and ongoing operations
3	Obsolescence	Agility and timing
4	Email Feature Set	Functionality
5	Other capabilities	Other features that don't relate to user's email feature set, but affect value, such as archiving and e-discovery
6	Security	Securing data, particularly protected health information (PHI)
7	Availability /Resiliency	Ability of users to use the capability. Fault tolerance.
8	Interoperability	Able to connect with adjacent VA systems such as the VA authentication system
9	IT Workforce Expertise	Ability of IT staff to manage a Cloud service instead of systems
10	Transition Costs	Financial costs for migrating to the new Cloud capability
11	Operating Costs	Financial costs for operating the service once the capability was in operation.
12	Workforce (FTEs)	VA Manpower required
13	Hosting Facilities	Amount of space required in VA datacenters
14	Acquisition & Funding	Timing, predictability, and type of funds
15	Mandate	Compliance with Federal laws, policy, and regulations

To answer question 1, the researchers compared the fifteen DFs used by the VA (see VA DF definitions above) to the nine USFCEF DFs described in Chapter 2 (listed on the right side Figure 37). This comparison, along with other supporting evidence, was used to determine whether the USFCDF DFs were necessary and sufficient for a Cloud migration decision.

Q1a - Were all of USFCDF Decision Factors necessary for the Cloud decision?

All of the USFCDF DFs would be found necessary if the VA applied each and every one of them in their Cloud migration decision. Because the VA used a different set of DFs

from the USFCDF, the VA DFs were mapped to the USFCDF DFs – as depicted in Figure 39.

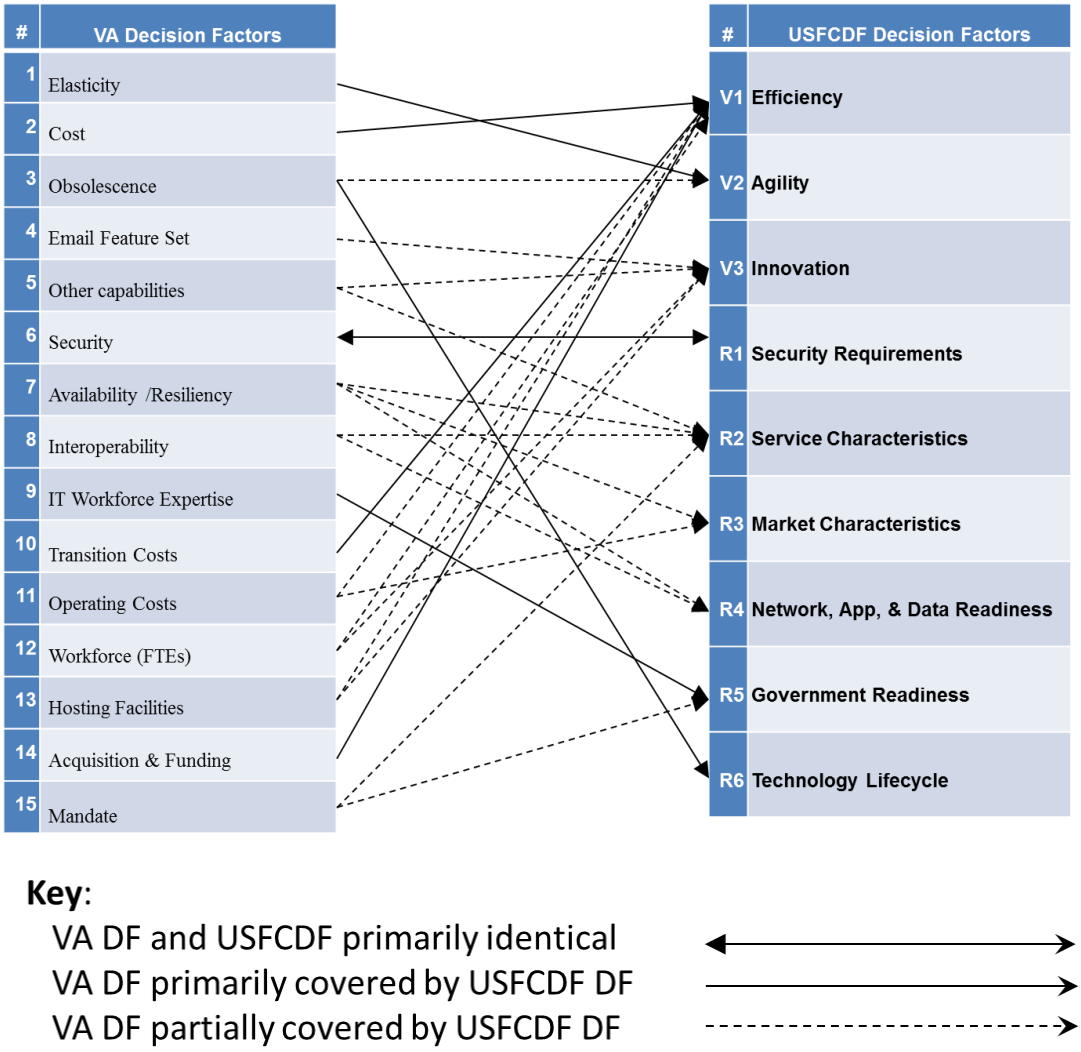


Figure 39 - VA DFs Mapped to USFCDF DFs

The arrows in Figure 39 designate, for each VA DF, the corresponding USFCDF DF(s). A double line suggests a near-identical correspondence – one to one (e.g. Security). A

one-way solid line indicates that the VA DF is primarily covered by the USFCDF. The dotted arrow indicates partial coverage by the corresponding USFCDF DF. In some cases, the VA DF is covered by more than one USFCDF. In that case, no single USFCDF provides full coverage for that particular VA DF. Note, unless a set of corresponding VA & USFCDF's are identical, a DF on one side may cover more than one on the adjacent side.

After mapping the VA DFs to the USFCDF DFs, the next step toward answering this first research sub-question is to apply set theory and determine whether the mapping of set of VA DFs to USFCDF DFs was surjective (also referred to as onto). USFCDF DFs are surjective if every element of the USFCDF is mapped to by at least one element of the VA set of DFs. The mapping of the VA DF's to the USFCDF was fully surjective at the time the VA made their critical decision for Cloud because the VA DF's used at the time of the decision covered all the USFCDF DFs. None of the USFCDF DFs were absent an incoming mapping arrow. Therefore all USFCDF DFs were necessary for the VA decision to migrate to Cloud.

This finding can be further validated by checking whether the lowest ranking USFCDFs were still considered necessary by those interviewed for this case. The interviewees were asked to rank the USFCDF DFs, and then asked whether any of the USFCDF DFs would not be of value (i.e. unnecessary) for their Cloud migration decision. Table 15 summarizes the rankings given the USFCDF DFs by those interviewed during the case study.

Table 25 - VA Ranking of USFCDF Decision Factors (By Three VA Decision Stakeholders)

VALUE RANKINGS					
Factor	**I1**	**I2**	**I3**	**AVG**	**Statements**
Efficiency	1	2	2	1.7	A wash. Everything we do has to have cost efficiency attached to it Cloud at times can actually cost you more money A little higher cost than what we could do internally
Agility	3	1	1	1.7	Attractive because the way we work in the government Frees us from funding and manning upgrades Don't have to build it all out, pay for it again. Unless you have agility, what really is the value?
Innovation	2	3	3	2.7	Could be a little bit of value The innovation component of email? I don't see it. It's like an outsource.
READINESS RANKINGS					
Factor	**I1**	**I2**	**I3**	**AVG**	**Statements**
Security	1	1	2	1.3	Security has to be there as the first concern Cost of "FISMA high" makes cloud impractical Security is a foundation. Otherwise there is no option.
Service Characteristics	2	2	5	3.0	A list of service characteristics is very, very important in the decision factor Without this, you don't have a game Record archiving is important
Market Characteristics	4	4	5	4.3	Need interoperability between vendors Long migrations preclude swapping vendors Will not swap out vendors very often
Net App Data Readiness	5	3	4	4.0	Need Resiliency and availability Need to trace problems end-to-end, no finger pointing Legacy data available to migrate
Government Readiness	3	6	3	4.0	For the user, shouldn't be an issue Some concern about job loss Lack IT staff with service, instead of systems, skills
Technology Lifecycle	6	5	1	4.0	Exchange 2003 and servers are seven years old The stuff needs to be replaced desperately. The timing for this particular migration is perfect

Innovation had the lowest average ranking among the three USFCDF value DFs. The comments made by the VA stakeholders indicated innovation was of little value for this

Cloud migration decision. If any of the three value DFs were unnecessary, based on the expertise of the three key stakeholders in the VA's Cloud migration decision, then it would have been the innovation DF. Yet, despite its low ranking, innovation was part to the VA's decision about migrating their email. Aspects of Innovation mapped to four VA DFs: email feature set (DF #4), other capabilities (DF #5), workforce (DF #12), and hosting facilities (DF #13).

In particular, Kundra indicates that innovation frees an organization from "being burdened by asset management." VA sought to move from owning systems and managing systems to managing services. This would free up much needed datacenter space. It would also permit them to reassign saved manpower to other priority initiatives, an important value because VA was constrained by a head count limit. Both of these VA factors align with the USFCDF innovation DF. Therefore, it can be concluded that agility, although the lowest ranked USFCDF value DF, was still important to VA.

Similarly, the USFCDF readiness DF the VA rated lowest, market characteristics, was also considered necessary by the VA for their Cloud migration decision. They included market characteristics in their projection by noting that there was sufficient competition to drive down future year costs. They also assessed the market to ensure that they could deploy their other IT systems that interoperated with email to a competitor's Cloud to avoid locking those future systems with the same vendor as their email.

As an additional investigation to determine whether all USFCDF DFs were necessary, the project lead for the Cloud migration decision maker was asked whether any DF was missing and he responded that he felt the USFCDF covered everything. (De Sanno 2012)

Given the finding that all the USFCDF DFs were necessary, the next sub-question considers whether the USFCDF lacked any DFs needed by the VA.

Q1b - Is the set of USFCDF decision factors sufficient?

This sub-question asks whether any DFs needed by the VA were missing from the USFCDF set of DFs. The set of USFCDF DFs would be found sufficient if together they incorporated all the factors considered by the VA. As noted earlier, the VA used a different set of DFs from the USFCDF. The same mapping in Figure 37 that was used to answer Q1a can also be applied to help answer Q1b. Again, set theory is applied, but this time analyzing the mapping coverage of the VA DFs by determining whether any VA DF lacks a mapping to a corresponding USFCDF DF.

As seen in Figure 39, all fifteen of the VA DFs were primarily covered by one or more of the USFCDF DFs. This can be seen by noting that each VA DF has one primary or multiple partial arrows mapping them to one or more USFCDF DFs. Therefore, the USFCDF DFs were sufficient to cover the concerns of the VA for their decision.

This conclusion was validated by questioning the Cloud migration decision maker whether any items were missing from the USFCDF. (De Sanno 2012) He stated that none were missing, but he did emphasize workforce and facility savings, suggesting that the USFCDF DFs would benefit from improved wording in their definitions that highlighted these two VA topics. The finding of the second sub-question is that yes, the USFCDFs were generally sufficient for the VA migration decision.

Q2. Does the USFCDF decision structure provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The second research question involves the USFCDF decision structure (DS). As noted earlier, a decision structure – such as the USFCDF DS or others – is simply a construct to organize individual DFs into categories or buckets of DFs, which provides decision makers a higher-level understanding of the elements of the decision. The first sub-question relates to DS's in general, and not specifically to just the USFCDF DF.

Q2a - Does a decision structure (in general) provide value?

To answer this sub-question, the researcher analyzed the VA Cloud migration decision to determine whether the VA applied a decision structure to marshal their DFs.

The VA applied a "pro-con" analysis to decide whether to migrate to migrate to Cloud. However, other than identifying whether a decision factor fell into the group of positives or negatives for migration, VA did not formally create a DS to marshal their DFs.

The VA's lack of formal DS would suggest that the VA did not find value from a DS. An alternative explanation is that the VA would have found value in a formal DS, but did not develop an explicit DS.

The conclusion from this case study research indicates that the VA would have found value in a DS had they developed a formal DS. The following observations support this conclusion:

1. The VA decision process was informal and lacked documentation leading to the decision and resulting from the decision. The DS was just one of many decision aids that could have been useful but were not adopted at that time. For example:
    a. De Sanno related that the decision was made during informal discussions between him and the VA CIO. (De Sanno 2015)

b. At the time of the decision, the only formal documentation was a white paper. (Susi 2012)

2. There is no evidence that the VA leveraged executive governance bodies in VA to review and make the decision. (De Sanno 2012) This limited the rigor and review of the decision. It also removed a driver for a D ; marshalling DFs to defend a position or to facilitate integration of new data for the decision. For example:
    a. A few senior IT leaders at VA "backed into the decision." (De Sanno 2015)
    b. The decision did not incorporate the concerns of some senior VA leaders beyond the IT leaders. The VA Office of Inspector General had concerns that subsequently caused the decision to be revisited and overturned. (Mazmanian 2014)
    c. The VA did not capture the decision in a formal decision document. No one interviewed could recall any formal decision document being signed. (Susi 2012) This is separate from the subsequent decision and approval for the VA to solicit bids from industry for a VA Cloud email contract.
3. The VA normally adopts a decision structure for significant IT decisions. (Landfried 2012) This suggests VA would have found value in applying a DS for the Cloud migration decision.

Given the value of a DS in general at the VA for IT decisions, and that evidences indicates that this Cloud decision did not benefit from a formal decision process, the answer to question Q2a is yes, the VA normally finds value in a DS, and likely would

have benefited from applying a DS to this Cloud migration decision, but did not adopt a DS because of the informal process used for the decision.

Q2b - Is the Value-Readiness paradigm of the USFCDF decision structure useful for marshalling decision factors?

The originator of the USFCDF declared that, "the logic and structure of the framework should be applicable for all agencies." (Kundra 2011) Therefore, this questions asks whether the VA Cloud migration decision suggests the value-readiness paradigm of the USFCDF decision structure is useful for marshalling decision factors (despite the VA not applying a DS to their decision beyond a simple pro-con structure)

There are some observations from this case that suggest the usefulness of the value-readiness paradigm:

1. VA applies a paradigm that incorporates cost and other values against risk when deciding about investment for new IT systems. Landfried stated this when discussing products that fell within her responsibilities. (Landfried 2012)
2. During testimony before the Senate about the Cloud migration, VA leadership testified that the success factors for the initial phase of the migration (the 15,000 mailbox pilot) would be determined using three metrics: Less Cost, SaaS [Cloud email] is Secure, and Transition [to Cloud email] is seamless. (Committee on Veterans' Affairs 2013) The first metric aligns with the USFCDF value dimension, and the third metric aligns with the USFCDF dimension of readiness (to migrate). The security metric is also an aspect of the USFCDF readiness dimension.

3. Twelve of the fifteen VA DFs DF's map align with either the USFCDF value dimension (8 DFs) or the USFCDF readiness dimension (4 DFs). Only three could not be cleanly categorized as either value or readiness as they contained elements of both. This suggests that, with minor changes to those three DFs (e.g. splitting some), the USFCDF value-readiness paradigm could serve to marshal the VA DFs. See Table 26.
4. The VA decision maker indicated after the decision that the VA decision would have benefited from marshalling his factors into aspects of a value-readiness paradigm, but noted that cost is always considered a major factor in Federal procurements. (De Sanno 2015)

Table 26 - VA Decision Factors: Alignment with USFCDF Value-Readiness Paradigm

#	VA Decision Factors	USFCDF Value?	USFCDF Readiness?	Split Alignment
1	Elasticity	✓		
2	Cost	✓		
3	Obsolescence			✓
4	Email Feature Set	✓		
5	Other capabilities			✓
6	Security	✓		
7	Availability /Resiliency		✓	
8	Interoperability		✓	
9	IT Workforce Expertise		✓	
10	Transition Costs	✓		
11	Operating Costs			✓
12	Workforce (FTEs)	✓		
13	Hosting Facilities	✓		
14	Acquisition & Funding	✓		
15	Mandate		✓	

The answer to sub-question 2b is that the VA case study indicates that a Federal IT leader would receive value in preparing for a cloud migration by adopting the USFCDF value-readiness paradigm as a starting basis for their decision structure. However, because the VA did not actually apply a DS to their decision, this finding was not considered conclusive.

Q3. Does the USFCDF decision question provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The third research question is about the decision question (DQ). The DQ represents what the decision maker should answer as the basis of his/her decision. This case study research investigates whether the USFCDF DQ is consistent with the type of DQ needed to make Cloud migration decisions in the Federal Government. The research consists of two sub-questions; one relating to regulations from the Federal Government in general and the other related to the VA's approach to their DQ.

Q3a. Is the USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions?

This question was answered in the Army case study summary. Nothing in this case study summary differs from that answer. Therefore, the finding for sub-question 3a remains that USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions.

Q3b. Is the USFCDF decision question consistent with the needs of the decision maker?

The VA complied with FAR by casting the Cloud migration DQ as an analysis of alternatives. Their DQ includes the status quo which is the legacy Microsoft Exchange email system hosted at VA at 32 locations nationwide. Instead of listing Cloud migration as the single alternative to the status quo, the VA identified two alternatives to the status quo. The VA DQ depicted as email options is summarized in

Table 29.

Table 27 – VA Decision Question, Depicted as Options (De Sanno 2012)

Email Option	Description	- Owner - Operator	Cloud? - Deployment Model - Delivery Model
1 Current VA Email	Use existing (legacy Microsoft) Exchange 2003 (with possible technology refreshes)	- VA - VA using contractors	Cloud? No
2 VA-Hosted MS 365	Consolidate email into four datacenters running MS 365 email	- VA & MS - VA using contractors	Cloud? Slightly - Private SaaS
3 Cloud MS 365	Purchase email from a vendor hosting MS 365 to government customers	- Vendor - Vendor	Cloud? Yes - Community - SaaS

Although the VA's Cloud migration decision was shaped independently of the USFCDF, the result was an extension of the USFCDF binary yes-or-no decision to an Analysis of Alternatives (AOA) with the status quo mapping to the USFCDF "no" alternative and multiple Cloud (and partial Cloud) alternatives mapping to the USFCDF "yes" alternative. Although this approach would have enabled the VA to be compliant with FARs while also considering competing Cloud solutions for their Cloud migration, the lack of any formal decision committees and documents suggests that FAR-compliance was not a driver for the VA's DQ.

The answer to question 3b is that the USFCDF DQ is consistent with the needs of the Federal IT decision maker by extending the binary yes-or-no USFCDF DQ to an analysis of alternatives that includes the status quo.

Q4. Is email a well-defined legacy IT system?

The fourth research question inquires about whether email represents a well-defined legacy system across the Federal Government. A well-defined system is indicated when its functionality and system quality attributes are well known and documented and often implemented by competing IT vendors. This is in contrast to unique, proprietary systems that would require a Federal Agency to capture a list of functional requirements and system quality attributes. Furthermore, a legacy system that is not well defined is not likely to have competing vendors providing similar capabilities that would be exchangeable with the legacy system. If email is found to be a well-defined legacy system, then it can be argued that the results of this research project could be generalized to other well-defined legacy IT systems across the Federal Government.

This case researched two sub-questions, one questioning whether the VA's legacy email system (the status quo) was well-defined, and the other about whether email was widespread across the VA.

4a. Are email systems in the Federal Government defined by a small set of similar legacy commercial products?

The VA defined its email requirements based on the functionality provided by the current industry version of its legacy email system; Microsoft 2010 offered under a usage license as Microsoft 365. Any replacement to the VA legacy system, Cloud or otherwise, was expected to deliver the capabilities equivalent to the next version of Microsoft Exchange. This can be seen from the decision stakeholder's comments about the USFCDF Innovation DF in Table 24. Perhaps the most insightful observation is that when the VA asked industry for their feedback about providing Cloud email in their Request for

Information, VA used MS 365 as the reference for the functionality they required. (VA 2011)

Even had the VA Cloud email needs not been described as the upgraded version of its legacy email system, the needs would have also been well-defined by the email desktop client used in VA (Microsoft Outlook) The functionality and interoperability of Outlook defines the capabilities required of the Cloud email.

The answer to question 4a is that the VA had only one primary legacy system and one user interface. Therefore, they considered their legacy system well-defined.

4b. Is email used across the Federal enterprise?

This case study indicated that email was used across the VA enterprise. (VA 2011)

Q5. Would Cloud migration decision-makers have benefited from prior-knowledge of a validated USFCDF?

VA often leverages the experience of other Federal Agencies for their IT decisions. For example, the VA knew that two other Federal Agencies (Department of Agriculture and General Services Administration) had already migrated to Cloud email so VA reached out to gain insights from those two trailblazers. Note, VA felt that it did not need to wait for first-movers, and that these two agencies were much smaller than the VA Cloud migration effort. (De Sanno 2012) VA also tapped outside experts, such as Gartner, Inc., a leading information technology research and advisory company under contract with the VA. (Susi 2012) This indicates that the VA would value a validated USFCDF to gain insights from it for their own Cloud migration decision.

It's also likely the VA would have benefited from adopting a validated decision framework such as the USFCDF for their decision. As indicated earlier, the VA did not

formally document their Cloud migration decision other than through a whitepaper. Prior knowledge of a validated USFCDF would have helped document the decision, and provide a basis to defend the decision and answer inquiries about the decision.

An externally validated Cloud decision framework would provide the VA IT leadership with greater validity in demonstrating the value and readiness of VA to move to Cloud. Most telling is that the VA Cloud migration decision maker indicated that a framework such as the USFCDF would have been useful early in the decision process. (De Sanno 2015) The culture and actions of the VA related to IT decisions indicate that the answer to Q5 is yes, the VA Cloud migration decision-makers would have benefited from prior knowledge of a validated USFCDF.

Other Findings and Observations

In addition to findings directly related to the five research questions and their sub-questions, this investigation identified other observations relevant to the research topic and that would be of interest to others investigating the topic of Cloud migration in the US Federal Government.

VA O1 - The decisions process and associated decision gates

The decision process proceed through a series of gates that started prior to the primary Cloud migration decision and extended into a pilot of a cloud migration email option. For example, the VA Cloud migration decision originated from an initiative to consolidate VA email into four datacenters. That decision evolved to one of exploring a Cloud option in addition to evaluating in-house hosting options. Prior to and then after the primary VA Cloud migration decision, VA re-evaluated options as VA needs

evolved. Eventually, the decision was reversed, using elements of the primary decision but arriving at different conclusions. This observation suggests that a USFCDF could be of value across the decision lifecycle and not just at the key Cloud migration itself.

VA O2 – Decision documentation

The absence of formal documentation about the early decision gates – and even from the decision that led to the implemented cloud migration – was apparent at the VA. This observation supports the value of having a common Federal decision framework to act as a template to collect the decision data prior to the decision, and to serve as the details for the formal decision memo itself. Not only did the circumstances of the case make this obvious, but the decision maker himself made the same observation during the case interviews.

VA 03 – Funding (CapEx and OpEx)

The VA felt that a key benefit of Cloud was that it changed the way IT systems would be funded for periodic software and hardware upgrades. IT modernization often competes poorly with other Agency priorities and with new IT initiatives. For example, the VA legacy email system was seven years old at the time of the VA's Cloud migration decision. The previous upgrade replaced hardware and software that was nine years old at the time. By moving to the Cloud, the cost of upgrades would be baked into the cost of the email service. While this implies that VA would still implicitly pay for the Cloud vendors upgrades, the costs would be spread over time and also over multiple Cloud customers. The VA's email would appear much more like electricity or water for

funding. It would be like a utility and be a "must pay" bill that could not be deferred to fund other VA efforts.

VA O4 –Federal guidance and Cloud migration

VA felt that the "Cloud First" mandate was an important factor for them migrating to Cloud. They listed Cloud migration as their first priority in response to the US Office of Management and Budget's request for Federal Agencies to identify legacy systems to migrate to Cloud. (OMB 2011)

The VA decision maker also indicated he felt such guidance created additional weight for migrating to Cloud. In a larger sense, migrating to Cloud has also become a matter of compliance with another piece of Federal regulation. This observation indicates that Cloud compliance should be considered for incorporation into the USFCDF, either through an additional DF, or by expanding the scope of an existing USFCDF DF to incorporate compliance with emerging Federal mandates.

VA O5 – Shifting Responsibility to Cloud Vendors

Much has been written about how migrating to Cloud shifts an organizations mindset from owning systems to managing services. (Kundra 2011) For the VA IT leadership, an important subtly of this was that responsibility for email availability would rest on the IT vendor and not on the IT organization. This would free the VA IT leadership from being the focus of blame and questions for system outages. This is not a trivial concern. During the first interview with De Sanno, we took a 15 minute break while he responded to an outage of the VA's conferencing system. Note, this observation does not indicate that Cloud would be any more reliable or available than the VA's hosted email, but rather

that the responsibility for that reliability and availability would fall upon an external vendor instead of the VA's IT shop.

VA O6 – Cloud efficiencies are not limited to cost savings

The VA had goals to reduce the number of datacenters it owned or managed. VA also was struggling to improve service to Veterans with a cap on the number of personnel they could hire. By migrating to Cloud, VA felt they might save not only money, but also facilities and manpower. The USFCDF would benefit by broadening the definition of the USFCDF efficiency DF to include benefits from saving all three types of resources.

Summary & Conclusions (Case 3 –VA Email)

The VA developed a decision framework that supports the value of the USFCDF for the VA IT leadership. All the USFCDF DFs were necessary. The set of USFCDF DFs was generally sufficient, but may benefit by improving the definitions of some of the USFCDF DFs. The USFCDF DS, with its value-readiness paradigm would appear to provide value to the VA but the VA did not apply a DS (other than pro-con) for their decision so this finding is not conclusive. The USFCDF DQ, a basic yes-or-no question, was extended by the VA to conform to acquisition regulations and allow the decision maker to choose from several Cloud options. This case found support for extending the findings for email to other well-defined legacy IT systems. Finally, this case suggests IT leaders will value a decision framework such as the USFCDF.

Case 4 – General Services Administration (GSA) - Partial

This case study summary provides the findings and observations surrounding the April 2010 decision by GSA to migrate their legacy email systems to cloud. The primary

decision maker was Casey Coleman, Chief Information Officer. A stakeholder and observer of GSA's IT decisions was Dave McClure who served as GSA's Associate Administrator for Citizen Services & Innovative Technologies. The investigations for this case followed the methodology described in Chapter 3, but with reduced depth as this was an abbreviated case study. GSA's champion for this research investigation was McClure. The investigative sources for the case included McClure.

Some GSA documentation, particularly public statements and acquisition documents about the Cloud migration, also informed this case study investigation. This case was of particular note because:

- GSA was the first Federal Agency to migrate email to the Cloud. (GSA 2010)
- GSA decided to adopt Google Mail, a public Cloud delivery model while most other agencies were not comfortable with public Cloud
- GSA had early experience with Cloud, having migrated web services to the Cloud the year prior
- GSA was growing their Cloud procurement expertise through preparation for a government-wide contract for Cloud services
- GSA was leading the Government-wide security standard that was later known as FedRAMP.

The next sections summarize the findings and observations from this case study.

Q1 - Do the USFCDF decision factors provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The GSA framed their Cloud migration decision around the business case factors required for major IT investments as laid out by the Office of Management and Budget (OMB) and that affected the Chief Information Officers (CIOs) of Federal Agencies such as GSA. Both the prior GSA decision to migrate web servers and this decision to migrate email to Cloud "… were business cases that were put together largely following the OMB guidelines for the investment process that CIOs have to defend." (McClure 2012) The elements of the OMB business-case formed a decision structure described in the answer to Q2.

To answer Q1, the interviewee ranked the USFCDF DFs and then provided data on whether each individual DF was applied in the GSA decision. The interview was augmented by a review of GSA documents for indications where USFCDF DFs were applied.

Q1a - Were all of the USFCDF Decision Factors necessary for the Cloud decision?

All of the USFCDF DFs would be found necessary if the GSA applied each and every one of them in their Cloud migration decision. Because the GSA used a different set of DFs from the USFCDF, the interviewee, McClure, ranked the USFCDF DFs and then provided data for each DF about its application to the GSA Cloud migration decision. This provided a cross walk analysis from USFCDF DFs to the GSA decision. Table 28 lists the USFCDF DFs, how they were ranked by McClure, and statements about how the USFCDF DFs related to the GSA Cloud migration decision.

Table 28 - GSA Ranking of USFCDF Decision Factors based on interview with McClure

VALUE RANKINGS			
Factor	**Rnk**	**Statements**	**Source**
Efficiency	1	Looking at hard dollar savings; budget under duress	Interview
		Describe investment's return on investment	OMB A-11
Agility	2	Absolutely more responsive	Interview
		Google updates its product sometimes every night	Interview
		Compared to buying and upgrading version to version	Interview
		Is scalable and flexible	OMB A-11
		Agile, secure, reliable, and cost effective cloud	GSA Press
Innovation	3	Get "stuff" on a mobile device you couldn't before	Interview
		Gain integrated apps with basic email	Interview
		Contribution to mission delivery or agency management	OMB A-11
		How the investment will achieve innovation	OMB A-11
READINESS RANKINGS			
Factor	**Rnk**	**Statements**	**Source**
Security	3	Security was a big issue; Security is always on the list	Interview
		All options require FISMA & 2-factor authentication	Interview
		PIV-enabled per HPSD-12 [security requirements]	OMB A-11
Service Characteristics	1	Included consideration for device integration	Interview
		Address requirements of mandates	OMB A-11
		Facilitates data extraction	OMB A-11
Market Characteristics	4	Definitely important; migration of archived email out of their environment and into a different environment	Interview
		So that we were not vulnerable to vendor lock-in	Interview
Net App Data Readiness	3	Included consideration for Blackberries	Interview
		GSA's web server migration to Cloud helped us here	Interview
Government Readiness	4	Nothing is straightforward in the IT area	Interview
		Lots of leadership from Director and executive team	Interview
		Cultural resistance is also a major challenge.	Testimony to Congress
Technology Lifecycle	2	Lotus notes expiring	Interview
		Needed to replace servers	Interview
		At critical decision point whether to modernize in-house	Interview
		Elimination or reduction of another IT investment\	OMB A-11

The statements in the table above indicate that all USFCDF DFs applied to the Cloud migration decision. Even the lowest ranked DFs (innovation, market characteristics, and

technology lifecycle) applied to the GSA Cloud migration decision. Therefore all USFCDF DFs were included in the GSA decision.

Given the finding that all the USFCDF DFs were necessary, the next sub-question considers whether the USFCDF lacked any DFs needed by the GSA.

Q1b - Is the set of USFCDF decision factors sufficient?

This sub-question asks whether any DFs needed by the GSA were missing from the USFCDF set of DFs. The set of USFCDF DFs would be found sufficient if together they incorporated all the factors considered by the GSA.

This was answered by reviewing all documents and McClure's interview transcript for any elements of the GSA decision that were not covered by the USFCDF DFs. None were discovered, indicating, albeit inconclusively, that GSA had not applied considerations to their decision that were not already included in the USFCDF set of DFs. This conclusion was validated by asking McClure whether there was anything else about GSA's decision that was not covered by the USFCDF DFs. He agreed that the USFCDF DFs covered the GSA decision, closing by saying "The list [of USFCDF DFs] hits the cross section of things that are really into the decisional mix of moving to Cloud." (McClure 2012)

The finding of the second sub-question is that yes, the USFCDFs were sufficient for the GSA migration decision.

Q2. Does the USFCDF decision structure provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The second research question involves the USFCDF decision structure (DS). As noted earlier, a decision structure such as the USFCDF DS or others is simply a construct to

organize individual DFs into categories or buckets of DFs, which provides decision makers a higher-level understanding of the elements of the decision. The first sub-question relates to DSs in general, and not specifically to just the USFCDF DF.

Q2a - Does a decision structure (in general) provide value?

To answer this sub-question, the researcher analyzed the GSA Cloud migration decision to determine whether the GSA applied a decision structure to marshal their DFs. McClure stated that the GSA applied a "business case" analysis to decide whether to migrate to Cloud with pros and cons assessed on each decision category. The business case structure for IT investments such as Cloud migration is outlined in OMB Circular A-11, "Preparing, Submitting, and Executing the Budget." Guidance in the A-11 includes decision rationale in the section titled "Major IT Business Case: IT Capital Asset Overview and Justification." This decision rationale forms a structure that marshals the individual factors related to the IT investment justification.

The GSA applied a decision structure based on OMB A-11 to their decision process. This DS provided value by being compliant with Federal regulations as well as categorizing the major areas they evaluated for the Cloud migration decision. Therefore, the answer to question 2a is that a decision structure provided GSA value.

Q2b - Is the Value-Readiness paradigm of the USFCDF decision structure useful for marshalling decision factors?

The originator of the USFCDF declared that "the logic and structure of the framework should be applicable for all agencies." (Kundra 2011) Therefore, this questions asks

whether the GSA Cloud migration decision suggests that the value-readiness paradigm of the USFCDF decision structure is useful for marshalling decision factors.

As noted earlier, the GSA applied the Federal business case framework to their Cloud migration decision. This framework is described in OMB Circular A-11. The A-11 contains sections that map well to the USFCDF value dimension. The A-11 also contains sections that map well to the USFCDF readiness dimension.

Thus, the answer to sub-question 2b is that the GSA case study indicates that a Federal IT leader would receive value in preparing for a cloud migration by adopting the USFCDF value-readiness paradigm as a starting basis for their decision structure.

Q3. Does the USFCDF decision question provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The third research question is about the decision question (DQ). The DQ represents what it is that the decision maker should answer as the basis of his/her decision. This case study research investigates whether the USFCDF DQ is consistent with the type of DQ needed to make Cloud migration decisions in the Federal Government. The research consists of two sub-questions, one relating to regulations from the Federal Government in general, the other related to the GSA's approach to their DQ.

Q3a. Is the USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions?

This question was answered in the Army case study summary. Nothing in this case study summary differs from that answer. Therefore, the finding for sub-question 3a remains that USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions.

Q3b. Is the USFCDF decision question consistent with the needs of the decision maker?

The GSA complied with FAR by casting the Cloud migration DQ as an analysis of alternatives. Their DQ includes the status quo which is the legacy Lotus Notes system. GSA identified one alternative to the status quo. With two alternatives – status quo or public Cloud, the GSA DQ mapped closely to the binary "Migrate/Do Not Migrate" USFCDF DQ. The GSA DQ is summarized in

Table 29.

Table 29 – GSA Decision Question, Depicted as Options (De Sanno 2012; McClure 2012)

	Email Option	Description	- **Owner** - **Operator**	**Cloud?** - **Deployment Model** - **Delivery Model**
1	Current GSA Email	Use existing Lotus Notes, with a technology refresh.	- GSA - GSA using contractors	Cloud? No
2	Google Gmail	Purchase email from Google	- Vendor - Vendor	Cloud? Yes -Public -SaaS

Although the GSA's Cloud migration decision was shaped independently of the USFCDF, the result was an extension of the USFCDF binary yes-or-no decision to an Analysis of Alternatives (AOA) with the status quo mapping to the USFCDF "no" alternative and Gmail mapping to the USFCDF "yes" alternative.

The answer to question 3b is that the USFCDF DQ is consistent with the needs of the Federal IT decision maker by extending the binary yes-or-no USFCDF DQ to an analysis of alternatives that includes the status quo.

Q4. Is email a well-defined legacy IT system?

The fourth research question inquires about whether email represents a well-defined legacy system across the Federal Government. This case researched two sub-questions, one questioning whether the GSA's legacy email system (the status quo) was well-defined, and the other about whether email was widespread across the GSA reflecting whether email represented an Agency –wide legacy system.

4a. Are email systems in the Federal Government defined by a small set of similar legacy commercial products?

The GSA defined its email requirements based on the functionality provided by the current industry version of its legacy email system – Lotus Notes. (McClure 2012)

McClure indicated that replacement to the GSA legacy system, Cloud or otherwise, was expected to deliver the capabilities equivalent to the next version of Lotus Notes.

He noted that Cloud migration for email was "treated as a strategic sourcing more than anything else," indicating that, like other commodity outsourcing decisions, the requirements for email were well-defined by legacy products.

The answer to question 4a is that the GSA had only one primary legacy system and they considered their legacy system well-defined.

4b. Is email used across the Federal enterprise?

This case study indicated that email was used across the GSA enterprise. (McClure 2012)

Q5. Would Cloud migration decision-makers have benefited from prior-knowledge of a validated USFCDF?

The GSA had just successfully migrated its web services to the Cloud, using Cloud Infrastructure as a Service for the servers and storage to power the web sites. This saved GSA about $1.5m per year. (McClure 2012) This gave them confidence to rapidly assess email and make the subsequent email migration decision. GSA's prior experience indicates that they are receptive to re-using a decision framework, as they largely did by leveraging their experience with the web migration decision for the cloud migration decision.

It's also likely that GSA would champion a Federal-wide decision framework such as the USFCDF. In testimony to Congress, GSA was seen leading other Government-wide (not just Agency wide) initiatives such as: (McLure 2011)

- Stand up contract vehicles for secure IaaS solutions[12].
- Create a government-wide marketplace for data center availability.
- Development of the Federal Risk Authorization Management Program (FedRAMP).

GSA's success with Cloud, their actions to initiate Government-wide Cloud procurement tools, and their own decision framework aligned with USFCDF together support the finding that the answer to Q5 is yes, the GSA Cloud migration decision-makers would have benefited from prior knowledge of a validated USFCDF.

[12] See Chapter 2 for a discussion on Infrastructure as a Service (IaaS)

Other Findings and Observations

In addition to findings directly related to the five research questions and their sub-questions, this investigation identified other observations relevant to the research topic and that would be of interest to others investigating the topic of Cloud migration in the US Federal Government.

GSA O1 – Successful Cloud experience encourages subsequent Cloud migration

GSA's decision to migrate email to the Cloud was influenced by their successful decision to migrate web services to the Cloud a year prior. This made them more likely to migrate well-defined systems to Cloud. Their web migration decision did not appear to add or subtract any DFs, but it did cause them to carefully evaluate the service characteristics DF. This can be seen by the importance GSA placed on this DF (GSA was the only case that ranked this DF #1). The importance of the service characteristics DF can also be found in the GSA's communications with industry. Their Request for Information (RFI) and subsequent Request for Proposal (RFP) both contained extensive sections outlining the integration and other non-functional requirements related to service characteristics. McClure note that "That's a big lesson learned [from migrating] … nothing is straightforward in the IT area," prompting them to focus on service characteristics to ensure the vendor supports the Cloud capability adequately and provides necessary interoperability with other systems and devices outside the Cloud.

GSA O2 – Adopting Public Cloud

GSA selected Gmail, a public Cloud offering. They felt that this offering had adequate security because it met the standards laid out in the Federal Information Security Management Act of 2002. "Security is always on the list because you just have to be

able to show compliance with the SIFMA process." (McClure 2012) Security was a threshold DF and public Cloud met this threshold. Once the security threshold was met, other decision factors came to the forefront. In particular, GSA strove to drive down costs. Public Cloud, because of economies of scale, provided such savings.

Summary & Conclusions (Case 4 – GSA Email)

The GSA case was a partial case researched to provide expand the findings from small Federal Agencies. The GSA applied a decision framework based on a OMB-directed business case and informed by a prior GSA Cloud migration. All the USFCDF DFs were necessary. The set of USFCDF DFs was sufficient. The USFCDF DS, with its value-readiness paradigm mapped to the business case categories and would appear to provide value to the GSA. The USFCDF DQ, a basic yes-or-no question, was tailored by the GSA to conform to acquisition regulations. This case found support for extending the findings for email to other well-defined legacy IT systems. Finally, this case suggests IT leaders will value a decision framework such as the USFCDF. This case observed how a prior Cloud migration decision and a PaaS deployment model affected the Cloud migration decision.

Case 5 – US Agency for International Development (USAID) - Partial

This case study summary provides the findings and observations surrounding the mid-2010 decision by USAID to migrate their legacy email systems to cloud. The primary decision maker was Jerry Horton, Chief Information Officer. The investigations for this case followed the methodology described in Chapter 3, but with reduced depth as this was an abbreviated case study. USAID's champion for this research investigation was

Horton. The investigative sources for the case included Horton as well as USAID documentation.

This partial case was of particular note because:

- USAID decided to adopt Google Mail, a public Cloud delivery model while most other agencies were not comfortable with public Cloud.
- USAID had early experience with Cloud, having migrated their conferencing system to Cloud.
- USAID operated from austere locations worldwide.
- USAID expedited the decision because of operational needs.

The next sections summarize the findings and observations from this case study. See the appendices for more background and context on this case.

Q1 - Do the USFCDF decision factors provide value to Federal IT leaders deciding whether legacy IT systems should migrate to the Cloud?

To answer Q1, the interviewee ranked the USFCDF DFs and then provided data on whether each individual DF was applied in the USAID decision. The interview statements were augmented excerpts from USAID documents related to the Cloud migration decision.

Q1a - Were all of USFCDF Decision Factors necessary for the Cloud decision?

All of the USFCDF DFs would be found necessary if USAID applied each and every one of them in their Cloud migration decision. Because USAID used a different set of DFs from the USFCDF, the interviewee, Horton, ranked the USFCDF DFs and then provided data for each DF about its applicability to the USAID Cloud migration decision. This provided a cross walk analysis from USFCDF DFs to the USAID decision Table 30 lists

the USFCDF DFs, how they were ranked by Horton, and statements about how the USFCDF DFs related to the USAID Cloud migration decision.

Table 30 - USAID Ranking of USFCDF Decision Factors based on interview with Horton

VALUE RANKINGS			
Factor	**Rnk**	**Statements**	**Source**
Efficiency	2	Hoping [Cloud] would not cost more [than legacy]	Interview
		More about performance than about cost	Interview
		We came back later and did a lot of the justifications	USAID Newsletter
Agility	3	Adding accounts needed to be easy	Interview
		Agility should also include device independence	Interview
		The agility aspect of it was huge	Interview
Innovation	1	Get out of email silos; not restricted to one site	Interview
		Availability while traveling in remote locations	Interview
		Google Apps came as an additional capability	Interview
		Easier to buy a service than to own & maintain	Interview
		One person to complain about when there is an issue	Interview
		Meet demands for secure access anywhere	USAID Newsletter
		Comply with OMB "Cloud First" mandate	USAID Newsletter
READINESS RANKINGS			
Factor	**Rnk**	**Statements**	**Source**
Security	1	Most important; predominant	Interview
		Be innovative, but don't get slapped down later	Interview
		Re-use USAID's prior Certification and Accreditation	Interview
		Must secure email in an international environment	Interview
		Improve security for increasingly mobile workforce	FCW Article
Service Characteristics	3	Had to be web based. That left only one option	Interview
		Scalable	Interview
Market Characteristics	5	Biggest issue [of this DF] for us was lock-in	Interview
		Want to be able to extract our information	Interview
Net App Data Readiness	4	Would allow USAID to use commercial networks	Interview
		Ended up being more complex than originally thought	Interview
Government Readiness[13]	6	Was not a factor at the time, but should have been	Interview
		Has proven very complex; change management	Interview
		IT staff was easy	Interview
Technology Lifecycle	2	We were going to have to spend a lot of money to refresh all of our email servers worldwide (85 sites)	Interview
		Separate lifecycles for servers, licenses, contractors	Interview

[13] USAID did not actually apply this DF to the 2010 decision, but with the benefit of hindsight stated it would have been of value to the decision maker. (Horton 2012).

The statements in the table above indicate that all USFCDF DFs except Government Readiness were considered as part of the Cloud migration decision. Horton indicated he neglected to consider it at the time but, based on lessons learned from the subsequent Cloud migration, sees value now in including government readiness in future Cloud migration decisions. Horton admitted that only two of the DFs were the primary drivers for the decision: innovation and security. (Horton 2012) However, even the lowest ranked DFs (agility and government readiness) applied to the USAID Cloud migration decision. Therefore all USFCDF DFs were considered necessary in the USAID decision. Given the finding that all the USFCDF DFs were necessary, the next sub-question considers whether the USFCDF lacked any DFs needed by the USAID.

Q1b - Is the set of USFCDF decision factors sufficient?

This sub-question asks whether any DFs needed by the USAID were missing from the USFCDF set of DFs. The set of USFCDF DFs would be found sufficient if together they incorporated all the factors considered by the USAID.

This was answered by reviewing all documents and Horton's interview transcript for any elements of the USAID decision that were not covered by the USFCDF DFs. None were discovered, indicating, albeit inconclusively, that USAID had not applied considerations to their decision that were not already included in the USFCDF set of DFs. This conclusion was validated by asking Horton whether there was anything else about USAID's decision that was not covered by the USFCDF DFs. He suggested nothing further. (Horton 2012)

The finding of the second sub-question is that yes, the USFCDFs were sufficient for the USAID migration decision.

Q2. Does the USFCDF decision structure provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The second research question involves the USFCDF decision structure (DS). As noted earlier, a decision structure such as the USFCDF DS or others is simply a construct to organize individual DFs into categories or buckets of DFs, which provides decision makers a higher-level understanding of the elements of the decision. The first sub-question relates to DSs in general, and not specifically to just the USFCDF DF.

Q2a - Does a decision structure (in general) provide value?

To answer this sub-question, the researcher analyzed the USAID Cloud migration decision to determine whether the USAID applied a decision structure to marshal their DFs.

Horton indicated that the driver for the migration was "secure access [to email] anytime, anywhere." (USAID 2011) In his interview, he indicated that other factors were secondary. Horton's statement represents the two dimensions of the USFCDF; value (access anytime, anywhere) and readiness (secure). As Horton related how other USFCDF factors related to his decision, he reiterated that this was primarily about the value achieved through the innovation of worldwide access as long as the Cloud service had readiness. He subsequently validated the vendor's security readiness by using the security and accreditation recently accomplished by GSA for their Cloud migration. Therefore, the answer to question 2a is that a decision structure provided USAID value.

Q2b - Is the Value-Readiness paradigm of the USFCDF decision structure useful for marshalling decision factors?

The originator of the USFCDF declared that, "the logic and structure of the framework should be applicable for all agencies." (Kundra 2011) Therefore, this question asks whether the USAID Cloud migration decision suggests that the value-readiness paradigm of the USFCDF decision structure is useful for marshalling decision factors.

As noted earlier, the USAID focused on the value of worldwide access and the security readiness of the Cloud provider. This fits the value-readiness paradigm.

Thus, the answer to sub-question 2b is that the USAID case study indicates that a Federal IT leader would receive value in preparing for a cloud migration by adopting the USFCDF value-readiness paradigm as a starting basis for their decision structure.

Q3. Does the USFCDF decision question provide value to Federal IT leaders deciding whether legacy IT systems should migrate to the Cloud?

The third research question is about the decision question (DQ). The DQ represents what it is that the decision maker should answer as the basis of his/her decision. This case study research investigates whether the USFCDF DQ is consistent with the type of DQ needed to make Cloud migration decisions in the Federal Government. The research consists of two sub-questions, one relating to regulations from the Federal Government in general, the other related to the USAID's approach to their DQ.

Q3a. Is the USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions?

This question was answered in the Army case study summary. Nothing in this case study summary differs from that answer. Therefore, the finding for sub-question 3a remains

that USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions.

Q3b. Is the USFCDF decision question consistent with the needs of the decision maker?

USAID complied with FAR by casting the Cloud migration DQ as an analysis of alternatives. Their DQ includes the status quo, the legacy Microsoft Exchange systems maintained at 85 locations globally. USAID identified an alternative to the status quo – public Cloud. With two alternatives – status quo or public Cloud, the USAID DQ mapped closely to the binary "Migrate/Do Not Migrate" USFCDF DQ. The USAID DQ is summarized in

Table 31.

Table 31 – USAID Decision Question, Depicted as Options (Horton 2012)

Email Option	Description	- **Owner** - **Operator**	**Cloud?** - **Deployment Model** - **Delivery Model**
1 Current USAID Email	Use MS Exchange with a technology refresh.	- USAID - USAID w/ contractors	Cloud? No
2 Google Gmail	Purchase email from Google	- Vendor - Vendor	Cloud? Yes - Public - SaaS

Although the USAID's Cloud migration decision was shaped independently of the USFCDF, the result was an extension of the USFCDF binary yes-or-no decision to an

Analysis of Alternatives (AOA) with the status quo mapping to the USFCDF "no" alternative and Gmail mapping to the USFCDF "yes" alternative.

The answer to question 3b is that the USFCDF DQ is consistent with the needs of the Federal IT decision maker by extending the binary yes-or-no USFCDF DQ to an analysis of alternatives that includes the status quo.

Q4. Is email a well-defined legacy IT system?

The fourth research question inquires about whether email represents a well-defined legacy system across the Federal Government. This case researched two sub-questions, one questioning whether the USAID's legacy email system (the status quo) was well-defined, and the other about whether email was widespread across the USAID reflecting whether email represented an Agency–wide legacy system.

4a. Are email systems in the Federal Government defined by a small set of similar legacy commercial products?

USAID defined its email requirements based on the functionality provided by the current industry version of its legacy email system – Microsoft Exchange. (Horton 2012) Horton indicated that replacement to the USAID legacy system, Cloud or otherwise, was expected to deliver the capabilities equivalent to Exchange, although the user interface would look different and because it would be web-based.

The answer to question 4a is that the USAID had only one primary legacy system and they considered their legacy system well-defined.

4b. Is email used across the Federal enterprise?

This case study indicated that email was used across the USAID enterprise. (Horton 2012)

Q5. Would Cloud migration decision-makers have benefited from prior-knowledge of a validated USFCDF?

USAID had just successfully migrated its conferencing system to the Cloud, using Cloud Software as a Service through Adobe. This gave USAID confidence to rapidly assess email and make the subsequent email migration decision. USAID's prior experience indicates that they are receptive to re-using a decision framework, as they largely did by leveraging their experience with the conferencing decision for the cloud migration decision.

It's also likely that USAID would adopt a Federal-wide decision framework such as the USFCDF. USAID felt comfortable leveraging insights from others who adopted public Cloud, including a university and a health care provider. They also leveraged the security certification and accreditation USAID performed for their Cloud migration.

USAID's prior success with Cloud and their cultural acceptance of help from external organizations support the finding that the answer to Q5 is yes, the USAID Cloud migration decision-makers would have benefited from prior knowledge of a validated USFCDF.

Other Findings and Observations

In addition to findings directly related to the five research questions and their sub-questions, this investigation identified other observations relevant to the research topic and that would be of interest to others investigating the topic of Cloud migration in the US Federal Government.

USAID O1 – Successful Cloud experience encourages subsequent Cloud migration
USAID's decision to migrate email to the Cloud was influenced by their successful decision to migrate conferencing to the Cloud a year prior. This made them more likely to migrate well-defined systems like email to the Cloud.

USAID O2 – Security is Relative
Most discussions about Cloud DFs suppose that Cloud could be less secure than email hosted in-house. Yet USAID felt that public Cloud would be more secure because it discovered that its employees abroad had used personal Cloud email (such as Gmail without enterprise security enhancements), digital stored files, and paper copies. These were all less secure than the Gmail deployment considered by USAID. In other words, moving to the Cloud was expected to provide better security than legacy email.

USAID O3 – Adopting Public Cloud
USAID selected Gmail, a public Cloud offering. They felt that this offering had adequate security because it met the standards laid out in the Federal Information Security Management Act of 2002. Security was a threshold DF and public Cloud met this threshold. Once the security threshold was met, other decision factors came to the forefront. In particular, USAID hoped Cloud email would not cost more than legacy email. After deployment, USAID found that Gmail (public Cloud), because of economies of scale, provided savings.

USAID O4 - The decisions process and associated decision gates
The decision process proceeded through a series of gates that started prior to the primary Cloud migration decision and extended into a pilot of a cloud migration email option. For example, the USAID Cloud migration decision originated from observing USAID

employees use Gmail. That led to exploring a Cloud option in addition to evaluating in-house hosting options. After the primary USAID Cloud migration decision, USAID initiated a pilot and was prepared to revisit the migration decision should the pilot not work out. This observation suggests that a USFCDF could be of value across the decision lifecycle and not just at the key Cloud migration itself.

USAID O5 – Decision documentation

The absence of formal documentation about the early decision gates, and even from the decision that led to the implemented cloud migration, was apparent at USAID. "I'm not sure that there ever was a formal decision," admitted Horton. The decision was formally documented later as part of the FAR guidelines for soliciting a vendor. Horton noted "There was a memo put to me that basically was part of the overall procurement package." This observation supports the value of having a common Federal decision framework to act as a template to collect the decision data prior to the decision, and to serve as the details for the formal decision memo itself.

USAID 05 – Cost and Efficiency

Although cost savings is highlighted in USAID's public rationale for the migration to Cloud, at the time of the decision, it was not very important. For example, the Cloud decision maker indicated he hoped it would cost about the same and not much more than the cost of his legacy system.

Summary & Conclusions (Case 4 – USAID Email)

The USAID case was a partial case researched to expand the findings from small Federal Agencies. All the USFCDF DFs were necessary, but only two were considered critical at the time – innovation and security. The set of USFCDF DFs was sufficient. The

USFCDF DS, with its value-readiness paradigm mapped to the innovation-security imperatives of the USAID decision. The USFCDF DQ, a basic yes-or-no question, was tailored by the USAID to conform to acquisition regulations. This case found support for extending the findings for email to other well-defined legacy IT systems. Finally, this case suggests IT leaders will value a decision framework such as the USFCDF.

In addition to the primary research questions, this case uncovered several observations about how a prior Cloud migration decision and a PaaS deployment model positively affected the Cloud migration decision. It also suggested that some early Cloud migration decisions were made without extensive rigor and associated documentation, suggesting a common decision framework, such as the USFCDF would have proven useful to USAID.

SYNTHESIS OF MULTIPLE CASE STUDIES

Introduction

This research project investigated whether the US Federal Cloud Decision Framework (USFCDF) will provide value to Federal IT decision makers determining whether their well-defined legacy IT systems should migrate to the Cloud. The research was accomplished through case studies of five US Federal Agencies that had decided to migrate their legacy email systems to the Cloud. The findings from each of those cases were summarized in the previous chapter. This chapter synthesizes and collectively analyzes the findings from those individual cases studies.

As seen in Table 11, the research spanned three full cases and two partial cases. The full cases met the criteria by Yin and Strake for triangulation through multiple diverse sources. The partial case studies were less robust, but provide insights that support generalization of the findings across different types of agencies (DoD and non-DoD) as well as across different system sizes (large and modest). For each case, both full and partial, the quantain bounding each case was the primary decision itself. In other words, the research focused on the Cloud migration decision and not the implementation or the eventual efficacy of the Cloud system.

The investigation into each case compared the components of the Agency's decision to that of the US Federal Cloud Decision Framework (USFCDF), which served as the unifying theory Yin recommended for case consistency.

Table 32 - Summary of Research Case Studies

Case		Replicative Logic Constants				Planned Variations	
Agency	Full/ Partial	Cloud Migration Decision	Legacy IT System	Delivery Model (SaaS)	Relatable to Theory	System Size	Agency Type
Army	Full	✓	✓	✓	✓	Large	DoD
NSF	Full	✓	✓	✓	✓	Modest	Non-DoD
VA	Full	✓	✓	✓	✓	Large	Non-DoD
GSA	Partial	✓	✓	✓	✓	Modest	Non-DoD
USAID	Partial	✓	✓	✓	✓	Modest	Non-DoD

In contrast to Chapter 4, which was organized by five case studies in sequence, this chapter is organized around the five research questions and sub-questions (these are repeated in Table 33 for quick reference).

Table 33 - Research Questions and Sub-questions

Main Body of Each Case Study Summary
1. Do the USFCDF **decision factors** provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?
a. Are all USFCDF decision factors necessary?
b. Is the set of USFCDF decision factors sufficient?
2. Does the USFCDF **decision structure** provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?
a. Does a decision structure (in general) provide value?
b. Is the Value-Readiness paradigm of the USFCDF decision structure useful for marshalling decision factors?
3. Does the USFCDF **decision question** provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?
a. Is the USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions?
b. Is the USFCDF decision question consistent with the needs of the decision maker?
4. Is email a well-defined legacy IT system?
a. Are email systems in the Federal Government defined by a small set of similar legacy commercial products?
b. Is email used across the Federal enterprise?
5. Would Cloud migration decision-makers have benefited from prior-knowledge of a validated USFCDF?

For each research question and sub-question listed in Figure 40, case study findings from Chapter 4 are synthesized to derive a strongly supportable answer. This approach this chapter uses for each subquestion can be seen graphically as a Wigmore inference diagram. Figure 1 provides a graphic example of the synthesis approach for subquestion 1a.

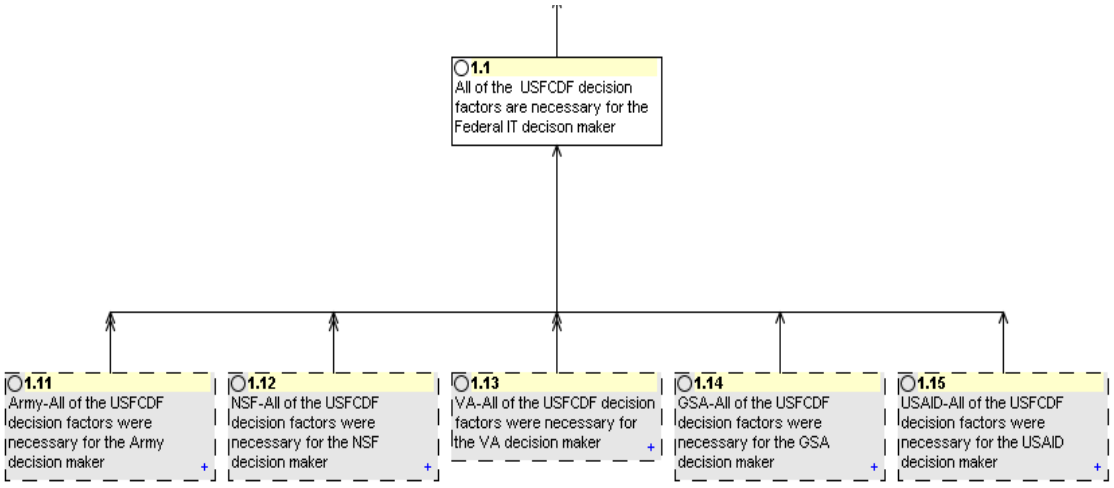


Figure 40 - Composition of typical subquestion analysis using Wigmore diagramming

After synthesizing the findings for each question and subquestion across all five case studies, this chapter closes with a synthesis of other observations discovered during the case study research that, although not directly applicable to the research questions, are of interest to the broader research area about Cloud migration in the US Federal Government.

Note: See Chapter 6 for the application of research answers from this Chapter to the research hypothesis and sub-hypothesis that originally shaped this research project.

Q1 - Do the USFCDF decision factors (DFs) provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

Nine USFCDF decision factors (DFs) represent the topics Kundra proposed Federal IT leaders consider for migrating their legacy IT systems to the cloud. Kundra marshalled these DFs into a decision structure (DS) consisting of two dimensions: value and

readiness. Table 34 provides a quick reference to these USFCDF DFs, paraphrasing the descriptions from Kundra in the US Federal Cloud Computing Strategy.

Table 34 - USFCDF Decision Factors Derived from Federal Cloud Computing Strategy (Kundra 2011)

Description	
Factor	**VALUE DFs (Is it a good idea to move to the Cloud?)**
Efficiency	Lower costs. Cloud provides economies of scale that should reduce costs. Cloud may also change the nature of costs from upfront capital expenses (CapEx) to ongoing operational expenses (OpEx). Suggests higher efficiency value for migrating legacy systems that have high per-user costs, low utilization rates, high maintenance expenses, or are fragmented (i.e. stovepiped).
Agility	Scalability and upgradability. Cloud provides value through rapid provisioning of computer resources – scaling up and down quickly; adding and cancelling users easily. Suggests higher agility value for migrating legacy systems that require long lead times to upgrade or increase/decrease capacity.
Innovation	New or better capabilities. Cloud can enhance customer satisfaction, usage/availability, and functionality. Suggests higher innovation value for migrating legacy systems
READINESS DFs (Can we do it and do it now?)	
Security	Vendor's compliance with security requirements. Cloud migrates data from a government facility to a vendor's facility where they typically support multiple customers. Federal Agencies must evaluate whether their vendors are ready to comply with Federal security guidance (Note: this predates FedRAMP, the government-wide security accreditation)
Service Characteristics	Vendor's performance and compliance. Cloud is still IT and performance requirements still apply, such as interoperability, availability, responsiveness, service & vendor reliability, administrative support, incident resolution, and compatibility with the Agency's larger architecture. In addition, Cloud must also comply with most Federal guidance affecting non-Cloud IT, such as records management (archiving, expunging, etc) and continuity of operations.
Market Characteristics	Vendor marketplace's maturity and breadth. Cloud is relatively new and the marketplace is evolving. Agencies should evaluate whether there is adequate competition (multiple vendors) for a procurement compliant with acquisition rules. Agencies should also evaluate whether the vendors use interoperable data formats so Agency data can be migrated to another vendor (or back to government) at some future time.
Net App Data Readiness	Agency's legacy application and infrastructure. Cloud migrates data and processing to a vendor's location outside the agency. Cloud will typically require more external bandwidth to the Agency. Data from the legacy application will likely need to be ported to the Cloud vendor, which may be difficult with some proprietary legacy systems. Also, other enterprise infrastructure such as desktop clients or interconnected Agency applications might not work when the legacy application is moved outside the Agency.
Government Readiness	Agency's culture and technical preparation. Cloud represents a shift from an internal system to an external service. This change may affect users and the jobs of the technical team. It will also require different technical expertise and often prerequisite action by sister Agencies.
Technology Lifecycle	Timing driven by legacy environment. The timing of the Cloud migration might be affected by upcoming milestones related to current plans, such as: hardware refresh, software upgrade, support contract renewal, or pending regulations. This factor does not affect whether to migrate but when to migrate. Such future events might also identify potential spikes in future funding that an Agency could repurpose toward the onetime upfront cost of the Cloud migration itself.

To answer whether the USFCDF DFs proposed by Kundra provide value to Federal IT leaders, each USFCDF DFs should be necessary and the set of USFCDFs should be sufficient for deciding whether a legacy IT system should migrate to the Cloud

Q1a - Are all of USFCDF Decision Factors necessary?

All of the USFCDF DFs would be found necessary if each and every one was needed, even marginally, for Cloud migration decisions. To determine whether all the USFCDF DFs were necessary, the researcher attempted to perform three tests for each case. This section reviews these tests and synthesizes the results.

For Q1a, the research project applied three tests to each case, each with a description of what was being measured and how the measurement would be evaluated. See Table 35 for a summary of these three tests for Q1a.

Table 35 - Tests for Q1a

Tests for Question 1a	
Test	**Measure & Metric**
1. Surjection	Measure. Obtain the criteria used by the Agency to make the Cloud migration decision and then map each Agency criterion onto the set of USFCDF DFs
	Metric: Each USFCDF aligned with at least one criterion used by the Agency (conversely identify any USFCDF DF not relevant to the decision)
2. Worst Case	Measure. Ask the Agency to rank the importance of the USFCDF DFs. Further investigate the lowest ranking value and readiness DFs to assess whether they provided any significant value
	Metric: The lowest ranking value DF and lowest ranking readiness DF were both relevant to the Agency's decision
3. Testimonial	Measure. Note cases where interviewees in a case state that all DS factors apply.
	Metric: Validating statement (conversely, negating statement)

In chapter four, these tests were applied and the results described in the narrative to determine the weight of evidence of each case toward answering question 1a. This can be seen graphically in a Wigmore inference diagram. For example, see the graphic application of these three test for the Army case study in both Figure 41 and Figure 42.

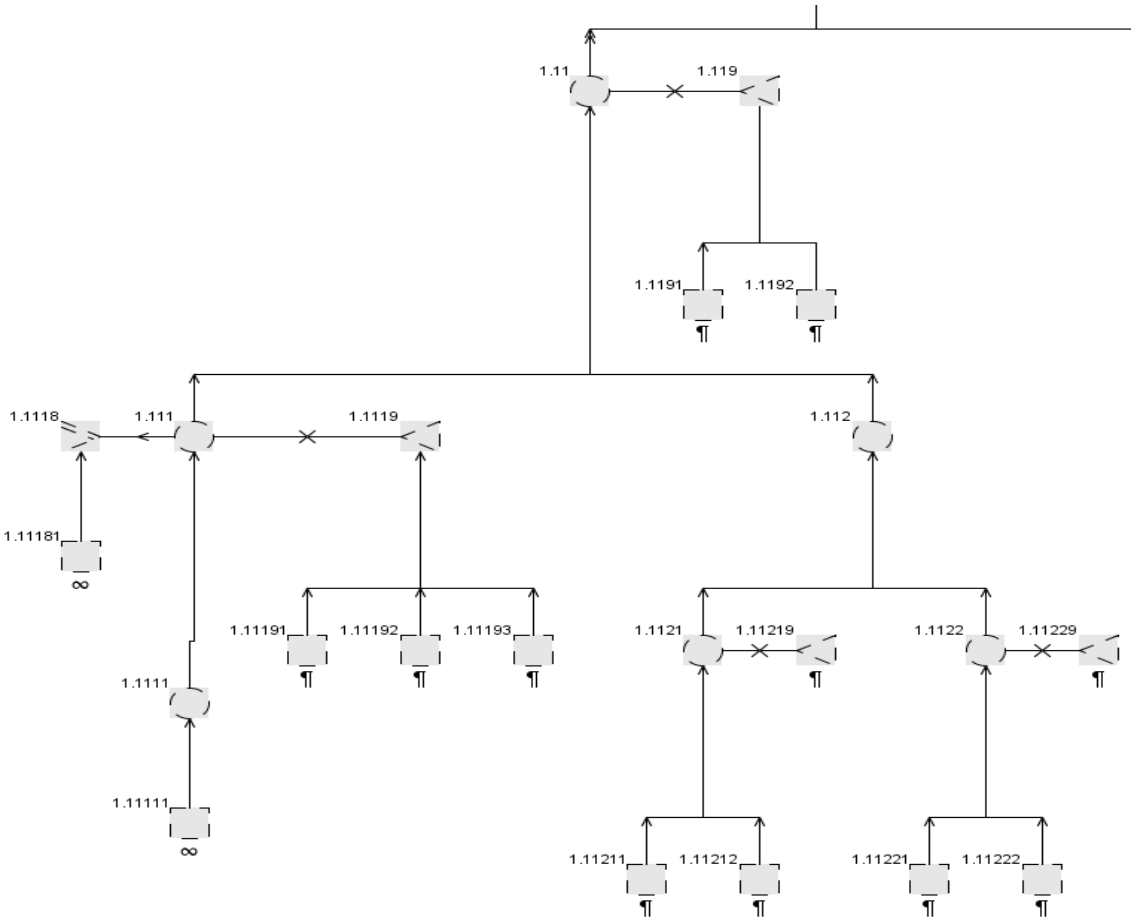


Figure 41 - Graphic of three Q1a tests for Army case (without descriptions)

In both Figure 41 and Figure 42, the top node, #1.11 depicts the weight of evidence toward Q1a from the Army case. The two subordinate nodes, #1.111 and #1.112

represent the weight of evidence from test 1 and test 2 respectively. The node adjacent to the top node represents the corroborative weight from test 3. Note, Figure 41 and Figure 42 represent the same Wigmore inference diagram, the first without text and the second with text. This case investigated eight subquestions and one final question across five cases. This produced 45 such graphics, as well as additional inference connections linking them to each other and in support to the overall hypothesis. Furthermore, these diagrams are detailed and difficult to read in print. A few select examples of Wigmore inference diagrams are contained in this Chapter and in Chapter 5, but it is not practical to print them all as part of this report. They are available, however, to those interested by opening the dataset accompanying this paper and creating multiple views using the Araucaria tool described in Chapter 3.

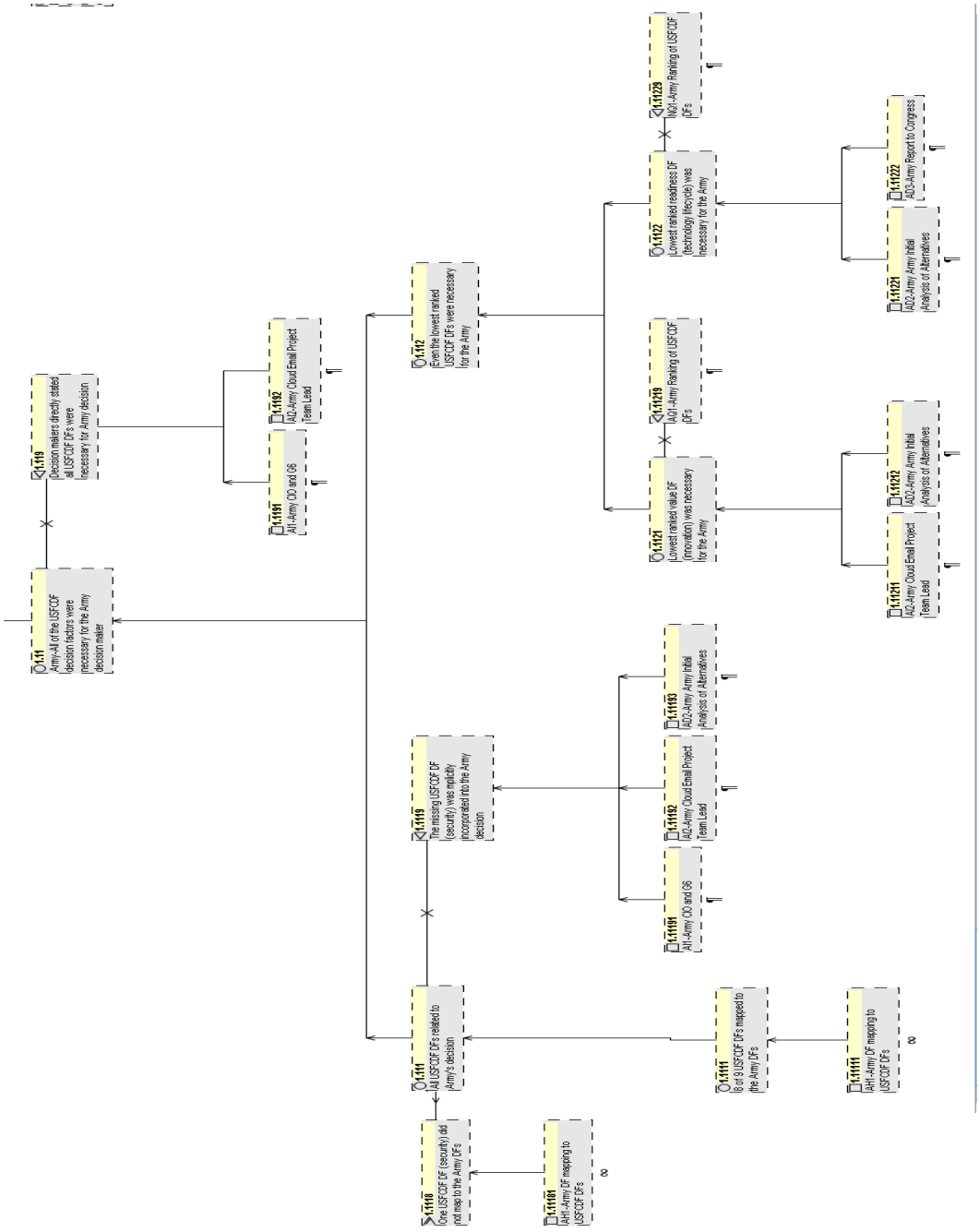


Figure 42 - Graphic of three Q1a tests for Army case (with text descriptions)

In cases where the basic metric identified an anomaly, that anomaly was investigated to ascertain its impact on the test result. A graphic example of such an anomaly is the

explanatory node and corroborative node adjacent to node 111. In this example, test 1 found an exception (node.1.1118 to the left), but this exception was explained through three sources and the conclusion supported (node 1.1119 to the right and three supporting nodes below it).

With the discussion above providing background, this analysis moves now to analyzing the Q1a test results from all five cases and synthesizing the results to answer Q1a. Table 36 summarizes the results of Q1a.

Table 36 - Test Results for Question 1a - Are all USFCDF Decision Factors Necessary?

Test Results for Q1a				
Test	**Case**	**Initial Score**	**Further Investigation[14]**	**Adjudicated Results**
1.Surjection	Army	?	Security DF assumed implicitly	↑↑
	NSF	?	Tech Lifecycle DF assumed implicitly	↑↑
	VA	↑		↑↑
	GSA	↑		↑
	USAID	?	Government Readiness DF, necessary in retrospect	↑
	Synthesis			↑↑
2.Worst Case	Army	↑		↑↑
	NSF	↑		↑↑
	VA	↑		↑↑
	GSA	↑		↑
	USAID	↑		↑
	Synthesis			↑↑
3. Testimonial	Army	X		XX
	NSF	X		XX
	VA	X		XX
	GSA	n/a		**n/a**
	USAID	n/a		**n/a**
	Synthesis			
KEY: ↑ Support ← Detracts X Corroborates ? Doubt n/a Not Accomplished (2= Strong)				

In Table 36, the initial score column represents the raw analysis. The next column, further investigation, strengthens or weakens the initial score resulting in the adjudicated score. The weighted result column adds additional weight for full case studies only. The full weight amplifies supporting, corroborating, or detracting adjudicated results – not just positive supporting results. Note that the first three cases were full cases. They carry more weight (represented by double arrows consistent with Wigmore diagraming

[14] See the respective case study summary in Chapter 4 for elaboration

showing strong support) than the two partial cases (represented by a single arrow showing support) in the weighted results.

The test results above indicate that test 1 (Surjective mapping between case DFs and USFCDF DFs) initially found two cases in support and three in doubt. Further investigation, as documented in Chapter 4, concluded that the USFCDF DFs initially discovered as missing from the Cloud migration decision were either assumed implicitly (Army & NSF) or were unintentionally omitted during the decision but subsequently considered to have relevancy (USAID). Furthermore, all three of the full cases provided testimonial from a stakeholder in the decision.

This synthesis of the five cases strongly supports the conclusion that the answer to Q1a is yes -- all of the decision factors proposed by Kundra in the USFCDF are necessary and therefore provide value to a Federal IT leader facing a decision on Cloud migration.

Q1b - Is the set of USFCDF decision factors sufficient?

The set of USFCDF DFs would be found sufficient if together they incorporated all the factors that provide value to a Federal Cloud migration decision. The USFCDF set of DFs would be suspect should it not cover significant factors these Agencies felt important in their Cloud migration decision.

To determine whether the set of USFCDF DFs were sufficient, the researcher attempted to perform two tests for each case. This section reviews these tests and synthesizes the results.

The two tests for Q1b are described in Table 37. Each test includes a summary of what was measured and how the measurement was evaluated.

Table 37 - Tests for Q1b

Tests for Question 1b	
Test	**Measure & Metric**
1. Surjection	Measure. Obtain the criteria used by the Agency to make the Cloud migration decision and then map each USFCDF DF onto the Agency DFs.
	Metric: Each Agency decision consideration aligned with at least one USFCDF DF (conversely no Agency decision consideration was missing from the USFCDF DFs)
2. Testimonial	Measure. Note cases where interviewees in a case state that the USFCDF DFs covered all Agency decision considerations
	Metric: Validating statement (conversely, negating statement)

In chapter four, these tests were applied and the results described in the narrative to determine the weight of evidence of each case toward answering question 1b. Again, this can be seen graphically in a Wigmore inference diagram. For example, see the graphic application of these two tests for the Army case study in both Figure 43 and Figure 44. As an additional investigation to determine whether all USFCDF DFs were necessary, interview transcripts were reviewed to identify interviewees who indicated that all USFCDF DFs were useful for a Cloud migration decision.

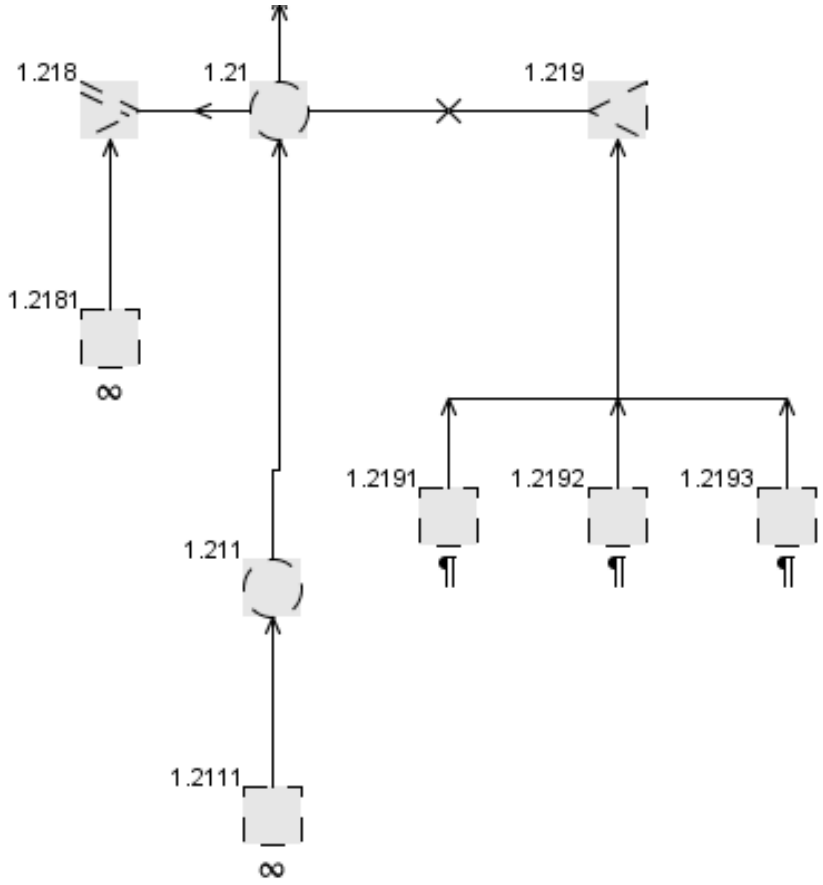


Figure 43 - Graphic of two Q1b tests for Army case (without descriptions)

Figure 43 and Figure 44 represent the same Wigmore inference diagram, the first without text and the second with text. In both Figure 43 and Figure 44, the top node, #1.21 depicts the evidence toward Q1b from the Army case. The subordinate node, #1.211 represents the evidence from test 1. The node adjacent to the top node represents the corroborative weight from test 2 (represented as node 1.2192) and two other sources as well. This example was provided because test 1 identified one minor shortcoming, therefore the investigation produced corroborative evidence suggesting the omission was minor and could be remedied though a wording change to the USFCDF DF. ,.

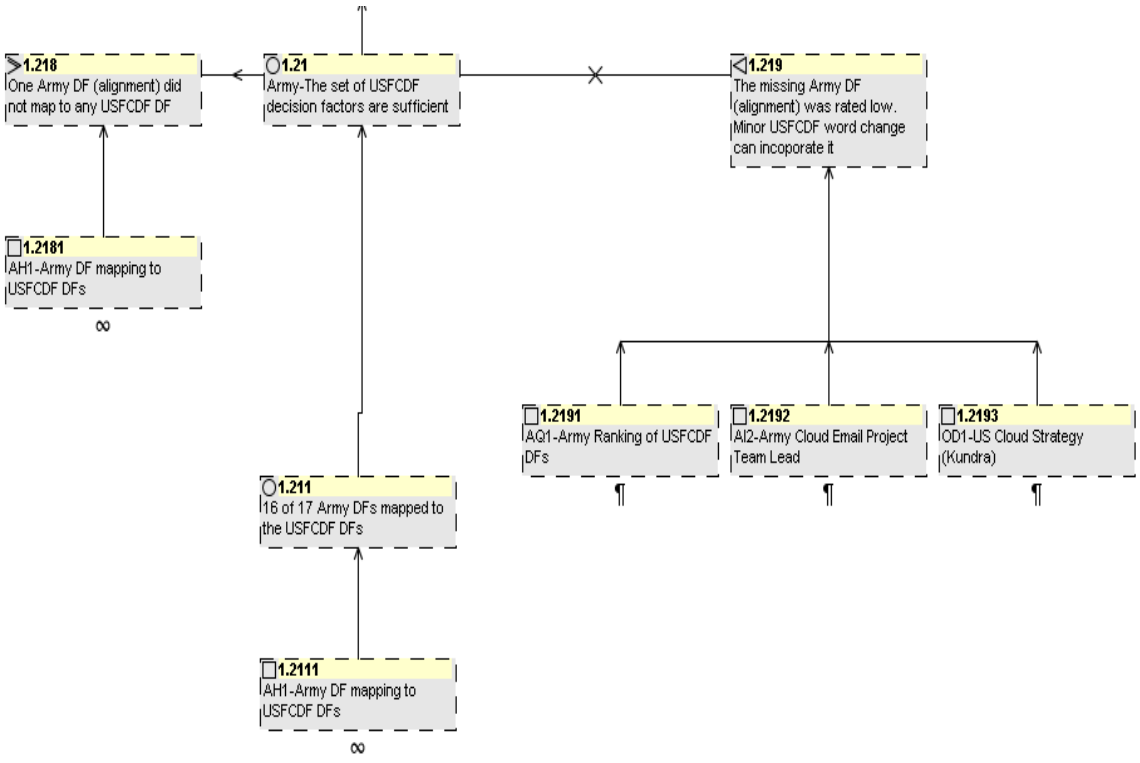


Figure 44- Graphic of two Q1b tests for Army case (with descriptions

With the discussion above providing background, this analysis moves now to combining the Q1b test results from all five cases and synthesizing the results to answer Q1b. The table below summarizes the results of Q2a.

Table 38 - Test Results for Question 1b - Is the set of USFCDF Decision Factors Sufficient?

Test Results for Q1b				
Test	**Case**	**Initial Score**	**Further Investigation[15]**	**Adjudicated Results**
1.Surjection	Army	?	Army "alignment with resources" minor	↑↑
	NSF	↑		↑↑
	VA	↑		↑↑
	GSA	↑		↑
	USAID	↑		↑
	Synthesis	X		↑↑
2.Testimonial	Army	↑		XX
	NSF	↑		XX
	VA	↑		XX
	GSA	**n/a**		**n/a**
	USAID	**n/a**		**n/a**
	Synthesis	X		XX
KEY: ↑ Support ← Detracts X Corroborates ? Doubt n/a Not Accomplished (2= Strong)				

This table follows the same logic and uses the same structure as Table 36 which was described in the Q1a synthesis previously and will not be overviewed here again.

But, the results related to Q1b merit discussion. The test results above indicate that test 1 (Surjective mapping between USFCDF DFs and the case DFs) initially found four cases in support and one in doubt. As noted in the discussion on the Wigmore diagrams for Q1b, the Army omission was minor, ranked low by Army, and arguably can be incorporated into the USFCDF with minor wording changes. The support from the surjection and the testimony from stakeholders in the three full cases strongly support the conclusion that the answer to Q1b is yes – the set of decision factors proposed by Kundra

[15] See the respective case study summary in Chapter 4 for elaboration

in the USFCDF are sufficient (with minor modifications) and therefore provide value to a Federal IT leader facing a decision on Cloud migration.

Q1 – Finding and recommendations

The synthesis from the five case studies strongly supported a "yes" answer to Q1a; all of the USFCDF decision factors are necessary. Similarly, this synthesis strongly supported a "yes" answer to Q1b; the set of USFCDFs are sufficient. Together, the results from Q1a and Q1b strongly support the answer to Q1 that yes, the USFCDF decision factors provide value to the Federal IT decision maker.

The synthesis for Q1 also identified the following recommendations related to Q1that would further enhance the USFCDF:

- Modify the set of existing DFs to include consideration for "alignment of resources with implementation." In other words, consider the availability (readiness) of funds for the migration effort in addition to the benefit (value) of the eventual efficiency from a successful migration to Cloud

Q2 - Does the USFCDF decision structure (DS) provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

In proposing the USFCDF, Kundra not only listed the nine decision factors (DFs) Federal Agencies should evaluate when considering Cloud migration, but he also marshalled those DFs into the two the DS dimensions of value and readiness.

Table 39 provides a quick reference to the two dimensions of the USFCDF DS, paraphrasing the descriptions from Kundra in the US Federal Cloud Computing Strategy.

Table 39 - USFCDF Decision Structure Derived from Federal Cloud Computing Strategy (Kundra 2011)

The Two Dimensions of the USFCDF Decision Structure		
Dimension	**Description & Associated USFCDF Decision Factors (DFs)**	
Value	**Description:**	The benefits of Cloud. Cloud provides economies of scale and imbedded inherent capabilities. This dimension of the USFCDF helps identify sources of value for a Federal Agency to consider when asking why to migrate a legacy system to the Cloud.
	Associated DFs	The three DFs this dimension contains are: Efficiency, Agility, and Innovation
Readiness	**Description:**	Ability to move to the Cloud in the near term. Agencies should make risk-based decisions which carefully consider the readiness of Cloud providers to fulfill their Federal needs as well as assess whether their Agency is ready to migrate soon.
	Associated DFs	The six DFs this dimension contains are: Security Requirements; Service Characteristics; Market Characteristics; Network Infrastructure, Application, and Data Readiness; Government Readiness, Technology Lifecycle. Note that the first three DFs related to the readiness of Cloud providers (who could be commercial or another Agency) while the last three relate to the readiness of the Agency considering Cloud.

To answer whether the USFCDF DS and its value-readiness paradigm proposed by Kundra provide value to Federal IT leaders, a DS (in general) should provide value for decisions. In addition, the value-readiness paradigm of the two DS dimensions should be useful for marshalling the DFs necessary for the Cloud migration decision.

Q2a - *Does a decision structure (in general) provide value*?

A DS would be seen as useful for Cloud migration decisions if the Agency decision stakeholders employed a DS and found it worthwhile. For this research, a DS was considered any mechanism the Federal Agency employed to categorize a larger set of decision factors, reducing the top level of the decision to 2-5 categories. Note, the narrower question about the usefulness of the specific USFCDF value-readiness paradigm for a DS is deferred to Q2b.

To determine whether a DS is useful for a Cloud migration decision, the researcher attempted to perform a single test for each case. This section reviews the test and synthesizes the results. The test for Q2a is described in Table 40. The test includes a summary of what was measured and how the measurement was evaluated.

Table 40- Test for Q2a

Test for Question 2a	
Test	**Measure & Metric**
1. Existence	Measure. Obtain the organizing construct for the decision factors used by the Agency to make the Cloud migration decision.
	Metric: The Agency applied a decision structure to their Cloud migration decision that proved useful to them.

In chapter four, these tests were applied and the results described in the narrative to determine the weight of evidence of each case toward answering Q2a. This case-level analysis can be seen graphically in a Wigmore inference diagram. For example, see the graphic application of these two Q2a tests for the NSF case study in Figure 45. (Q2a consists of only one simple test, so the simplified Wigmore diagram was not necessary to visualize the overall relationship of Q2a.)

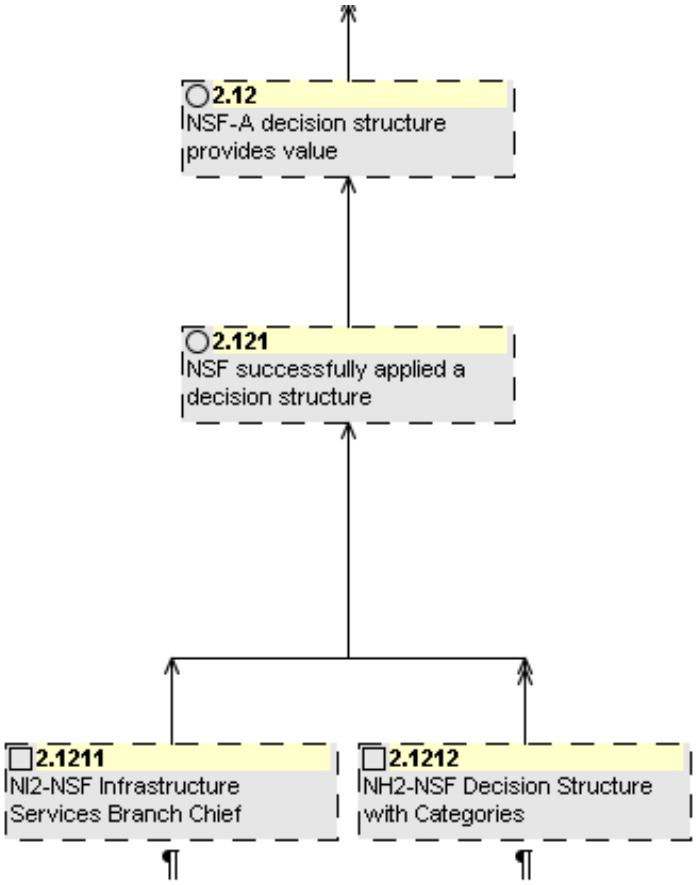


Figure 45 - Graphic of two Q2a tests for NSF case (with descriptions)

In both, the top node, #2.12 depicts the evidence toward Q2a from the NSF case. The lower nodes, #2.1211 and #2.1212 represent the two distinct pieces of evidence supporting the answer for Q2a in this case.

With the discussion above providing background, this analysis moves now to combining the Q2a test results from all five cases and synthesizing the results to answer Q2a. Table 41 summarizes the results of Q2a.

Table 41 - Test Results for Question 2a - Is a decision structure useful for Cloud migration decisions?

Test Results for Q2a				
Test	**Case**	**Initial Score**	**Further Investigation[16]**	**Adjudicated Results**
1. Existence	Army	🡅		🡅🡅
	NSF	🡅		🡅🡅
	VA	?	Usually apply DS for IT decisions. Did not in this case, but would in the future.	??
	GSA	🡅		🡅
	USAID	🡅		🡅
	Synthesis			🡅🡅
KEY: 🡅 Support 🡄 Detracts X Corroborates ? Doubt n/a Not Accomplished (2= Strong)				

This layout of the table follows the same logic and uses the same structure as Table 36, which was described in the Q1a synthesis previously and will not be overviewed here again.

But, the results related to Q2a merit discussion. The test results above indicate that test 1 (whether a DS was used in the Cloud migration decision) initially found four cases in support and one in doubt. As detailed in the VA case study summary in Chapter 4, the lack of a DS in this case was an abnormality for IT decisions made at the VA. Furthermore, the VA decision maker reflected in retrospect that a DS would have been useful. Although the VA was a major case and further research indicates VA finds value in applying a DS for IT decisions, the lack of a DS in the VA case weakens the strength of the VA result compared to the results from the other full case studies.

The general support from the cases strongly supports the conclusion that the answer to Q2a is yes, the USFCDF decision structure provides value to Federal IT leaders deciding

[16] See the respective case study summary in Chapter 4 for elaboration

whether a legacy IT system should migrate to the Cloud and therefore provides value to a Federal IT leader facing a decision on Cloud migration.

Q2b - Is the Value-Readiness paradigm of the USFCDF decision structure (DS) useful for marshalling decision factors?

The USFCDF DS would be found useful for marshalling decision factors if Agencies applied a DS similar to the USFCDF DS for their Cloud migration decisions.

This question was answered in two parts. The first part compared the USFCDF DF to the most widely accepted model for acceptance of new technologies, the Technology Acceptance Model (TAM). As described in Chapter 4, the two major categories in this model mapped well to the value-readiness paradigm of the USFCDF. The details of the analysis in Chapter 4 won't be repeated here except to say that TAM strongly supports a yes answer to Q2b.

The second part of the answer to Q2b results from synthesizing the five Cloud migration cases. Because the USFCDF DS was proposed after the decisions this paper researched were shaped, it is unlikely that any of those cases would have independently conceived a DS identical to the USFCDF DS. Therefore, this research evaluated the similarity between the DS used in each case and the value-readiness paradigm of the USFCDF DS.

To test whether the DS in a case aligned with the value-readiness paradigm of the USFCDF DS, the researcher attempted to perform two tests for each case. This section reviews these tests and synthesizes the results.

The two tests for Q2b are described in Table 42. Each test includes a summary of what was measured and how the measurement was evaluated.

Table 42 - Tests for Q2b

Tests for Question 2b	
Test	**Measure & Metric**
1. Definitional	Measure. Obtain the DS categories used by the Agency to make the Cloud migration decision and then compare the definition of each category to the value-readiness dimensions of the USFCDF DF
	Metric: Each Agency DS aligned with either value or readiness (conversely, discover no Agency DS description that relates to a consideration other than value or readiness.)
2. DF Mapping	Measure. Identify the DFs (or the subcomponents of the DS) for each Agency DS. Categorize the DFs by value, readiness, or other.
	Metric: The preponderance of the DFs in each DS map to either value or readiness. (conversely, the DFs in a particular DS do not correlate strongly with either value or readiness)

In chapter four, these tests were applied and the results described in the narrative to determine the weight of evidence of each case toward answering question 1b. Again, this can be seen graphically in a Wigmore inference diagram. For example, see the graphic application of these two tests for the Army case study in both Figure 46 and Figure 47.

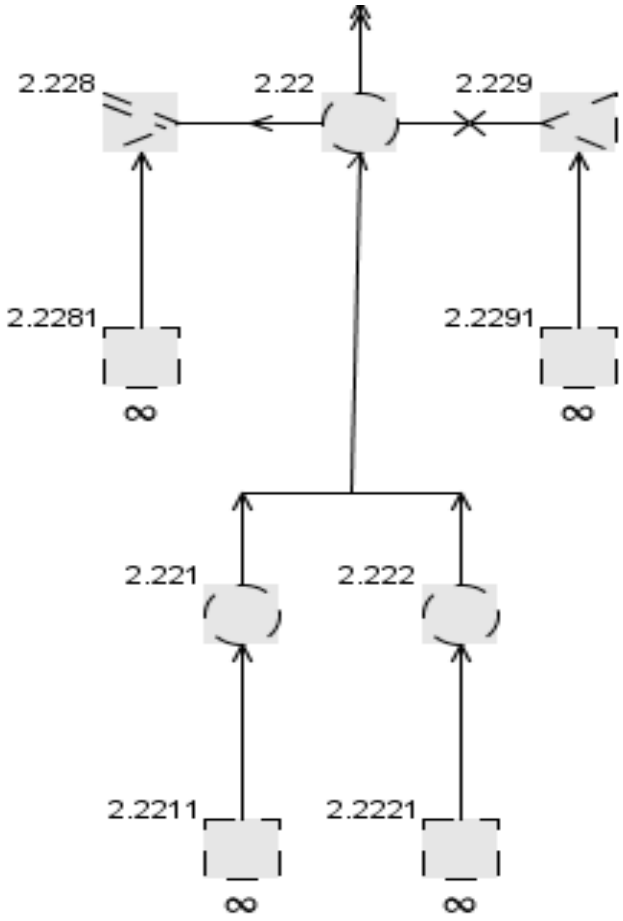


Figure 46 - Graphic of two Q2b tests for NSF case (without descriptions)

Figure 46 and Figure 47 represent the same Wigmore inference diagram, the first without text and the second with text. In both Figure 46 and Figure 47, the top node, #2.22 depicts the evidence toward Q2b from the NSF case. The subordinate nodes, #2.2211 and #2.2221 represent the evidence from tests 1 and test 2 respectively. Note that the intermediate inference node #2.222 suggests less support to #2.22 – At least one of the NSF DS categories failed test 2. This specific shortfall is represented by node #2.228.

Node #2.229 provides corroborative inference justifying why the conclusion in node #2.22 still remains valid.

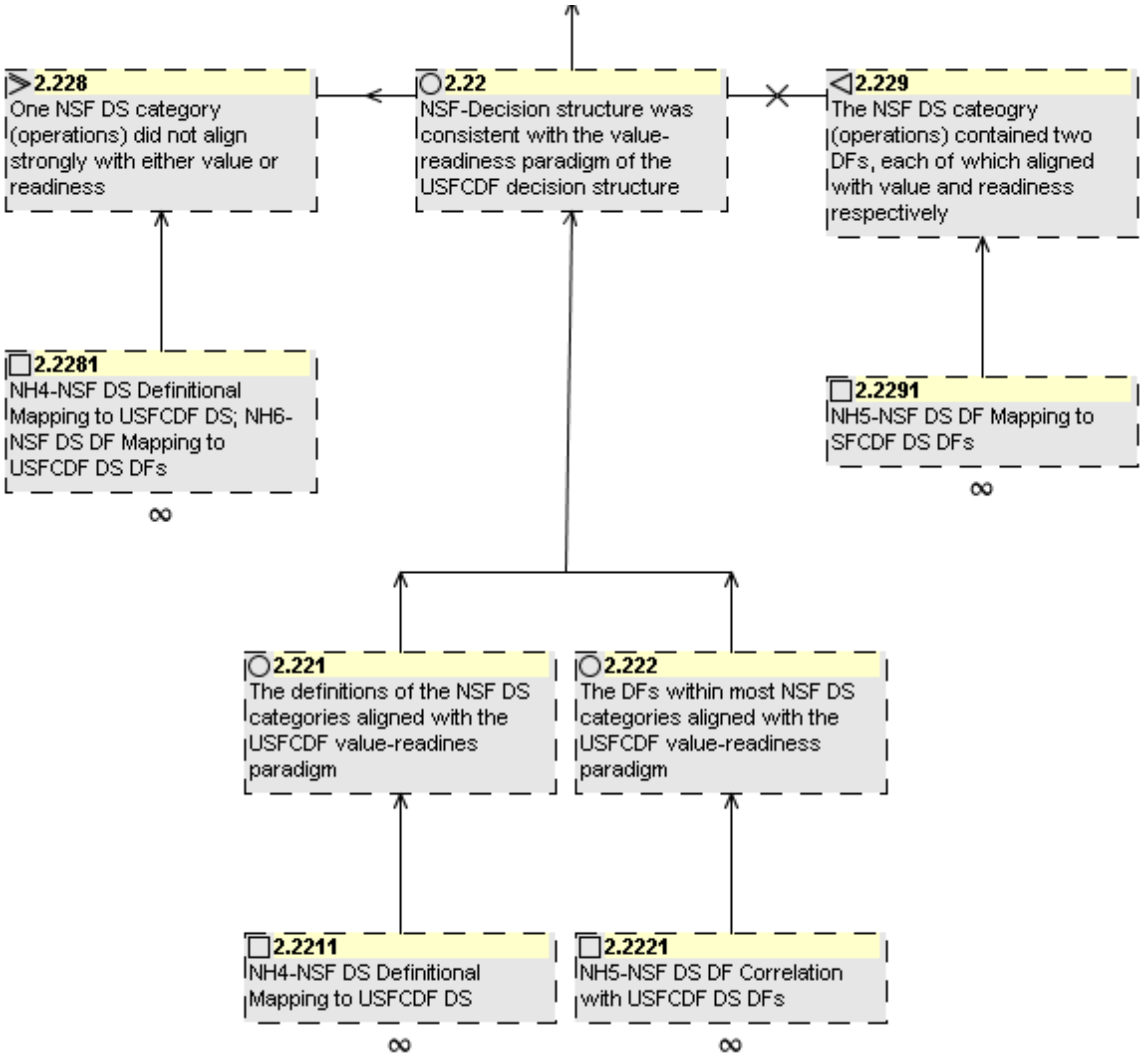


Figure 47- Graphic of two Q2b tests for NSF case (with descriptions)

This example from the analysis of Q2b in the NSF case was highlighted here because test 2 identified one minor shortcoming. Although the investigation produced corroboration

suggesting the omission was minor, this omission weakened support for Q2b from the NSF case.

With the discussion above providing background, this analysis moves now to combining the Q2b test results from all five cases and synthesizing the results to answer Q2b. The table below summarizes the results of Q2b.

Table 43 - Test Results for Question 2b – Is Value-Readiness paradigm of the USFCDF DS useful?

Test Results for Q2b				
Test	**Case**	**Initial Score**	**Further Investigation[17]**	**Adjudicated Result**
1.Definitional	Army	🡅		🡅🡅
	NSF	**?**	NSF Operations DS had split DFs. Weakens support	🡅
	VA	**?**	Usually apply DS for IT decisions. Did not in this case, but would in the future.	**?**
	GSA	🡅		🡅
	USAID	🡅		🡅
	Synthesis			🡅
2. DF Mapping	Army	🡅		🡅🡅
	NSF	**?**	NSF Operations DS had split DFs. Weakens support	🡅
	VA	**?**	Usually apply DS for IT decisions. Did not in this case, but would in the future.	**?**
	GSA	**n/a**		**n/a**
	USAID	**n/a**		**n/a**
	Synthesis			🡅
KEY: 🡅 Support 🡄 Detracts ✘ Corroborates ? Doubt n/a Not Accomplished (2= Strong)				

This table follows the same logic and uses the same structure as Table 36, which was described in the Q1a synthesis previously and will not be reviewed here again.

[17] See the respective case study summary in Chapter 4 for elaboration

But the results of Q2b merit discussion. The test results above indicate that test 1 (comparison of the definitions of the case's DS to the USFCDF value-readiness paradigm) initially found three cases in support and one in doubt. The investigation into the NSF was described earlier in reference to the two Wigmore diagrams, describing how one NSF DS category, operations, failed both tests because the adjudicated result was not as strong a support as in the Army's case. VA's situation was different. Although they usually apply a DS for major IT decisions, the VA made their Cloud migration decision informally and without the application of a DS. While this does not detract from the ultimate conclusion to Q2b, the VA case does not support the conclusion either.

The investigation into this subquestion also highlighted a minor shortcoming in the USFCDF regarding costs and efficiency. Cost has separate Federal reporting requirements and contains elements of both value and readiness. Federal guidelines require Agencies to report costs separate from other data about Cloud benefits such as agility and innovation. To simplify reporting after the Cloud migration decision, it would be helpful if the documentation for the decision (such as USFCDF documentation) aligned with subsequent reporting (that shows cost separately from other value DFs). Furthermore, although cost savings from Cloud clearly fall under the USFCDF value dimension, the decision makers for these five cases also analyzed costs required for the migration. If they did not have the funds for the migration surge, they could not migrate despite the future savings from ongoing the subsequent Cloud service.

In the final analysis for Q2b, the support from the definitional test and the DF mapping test supports the conclusion, albeit not as strongly, that the answer to Q2b is yes – the

value-readiness paradigm of the USFCDF is useful for marshalling DFs for a Cloud migration decision. The prior research into TAM, mentioned at the start of this section also provided strong support for a yes answer. Together, the test results and the TAM comparison suggest support that the answer to Q2b is yes. However, this analysis also suggests that the USFCDF DS would benefit from a cleaner separation in the value and readiness dimension to clarify the difference impact of migration vs ongoing operations.

Q2 – Finding and recommendations

The synthesis from the five case studies strongly supported a "yes" answer to Q2a; a decision structure (in general) provides value. This synthesis also supported a "yes" answer to Q2b, the value-readiness paradigm of the USFCDF decision structure is useful for marshalling decision factors. Together, the results from Q2a and Q2b moderately support the answer to Q2 that yes, the USFCDF decision structure provides value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud. The synthesis for Q2 also identified the following recommendations related to Q2 that would further enhance the USFCDF:

- Align the USFCDF DS to align with reporting required by OMB. This could be accomplished by expanding the scope of the USFCDF readiness dimension to include considerations for the cost of the migration itself.
- Improve the definitions of the USFCDF DS efficiency and readiness dimensions. In particular, better explain how the Cloud migration effort aligns with the readiness dimension

Q3 - Does the USFCDF decision question provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?

The third research question is about the decision question (DQ). The DQ represents what the decision maker should answer in his/her decision. In USFCDF, the overarching goal is to "Identify which IT services to move and when." (Kundra 2011) This implies that, for a specific legacy IT system, the USFCDF DQ asks "should this legacy system migrate to the Cloud?" The USFCDF DQ can be seen as a binary decision – migrate or do not migrate (yes or no). This is graphically depicted in Figure 48. Although the graphic decomposition appears trivial, it is provided here so that it can be compared and contrasted to the DQs used by the Federal Agencies to frame their DQ.

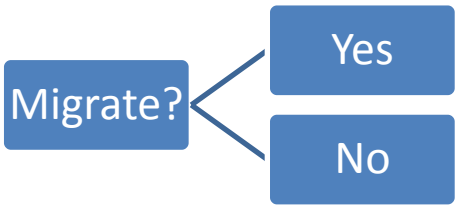


Figure 48 - Decomposition of Primary Part of the USFCDF DQ

To answer whether the USFCDF DQ proposed by Kundra provides value to Federal IT leaders, a DQ needs to be consistent with US Federal rules for IT acquisition and also serve the needs of the decision maker. Those are the subjects of Q3a and Q3b.

Q3a - Is the USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions?

A Federal Agency considering Cloud may source the Cloud services from either a commercial firm or another government agency. Although the requirements for a commercial procurement are more stringent than procurement from another government agency, the acquiring Agency must comply with Federal regulations in either case. Unlike commercial firms seeking Cloud services, Federal Agencies are bound by a complex set of regulatory guidance that describe, often in significant detail, what is required of a Federal IT leader for IT-related investments. Therefore, the elements of a Cloud migration decision, including the DQ, need to comply with this regulatory guidance.

The findings from Q3a research into nuances of government acquisition are reported in Chapter 4 under the Army case study summary. The key finding from this research is that, according to the Federal Acquisition Regulations (FARs), the Cloud decision question must be framed as an analysis of alternatives (AoA) with one of the alternatives being the status quo (i.e. the legacy system). Table 44 depicts this graphically.

Table 44- Federal Guidance for the DQ[18]

FAR DQ Alternatives	
DQ	Which alternative is best?
Choices	1. Status Quo
	2. Cloud

[18] Table is a graphic representation of guidance synthesized from the FARs, OMB A-11, and other sources

The research in Chapter 4 concluded that the USFCDF DQ is not inconsistent with Federal guidance and regulations. To better align with those requirements though, the USFCDF DQ can be recast similar to the FAR DQ with the alternatives for one DQ mapping to the other. This is shown in Figure 49.

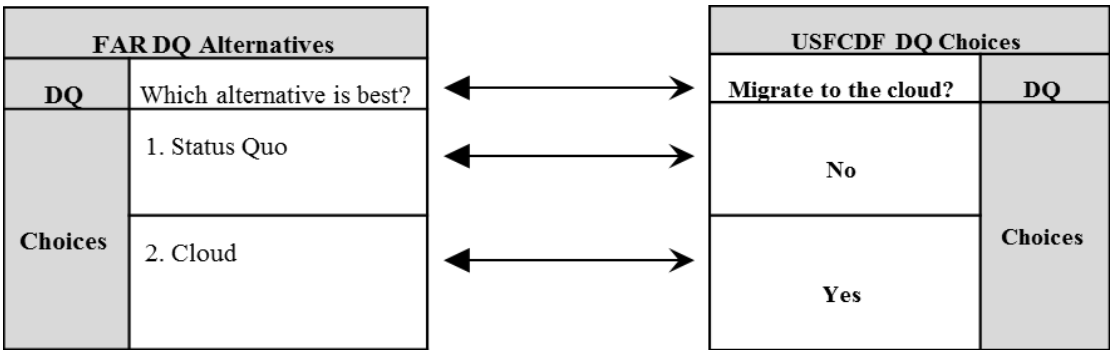


Figure 49 - Alignment of FAR DQ and USFCDF DQ

For the USFCDF DQ to be useful for an IT decision maker, it must be compliant with Federal guidance related to IT systems and IT procurement. This mapping shows the USFCDF DQ can be compliant when the UFCDF DQ choices are recast as alternatives. The answer to Q2a is a strong yes, the USFCDF decision question is consistent with US Federal guidance and regulations applicable to Cloud migration decisions.

Q3b - Is the USFCDF decision question consistent with the needs of the decision maker?

The USFCDF DQ would be considered consistent with the needs of the cloud migration decision maker if the cases applied a DQ that was found to be consistent with the USFCDF DQ. Based on the answer to Q3a, we can anticipate that the decision maker in

each case would have cast his or her DQ as an analysis of alternatives (AoA), having two alternatives (status quo and Cloud) and therefore consistent with the USFCDF DQ.

To determine whether the DQ in a case was consistent with the USFCDF DQ, the research project accomplished a single test for each case, inspecting each DQ and mapping it to the USFCDF DQ, as was done for the example in Figure 49.

The test for Q3b is described in Table 45. The table includes a summary of what was measured and how the measurement was evaluated.

Table 45 - Tests for Q3b

Tests for Question 3b	
Test	**Measure & Metric**
1. DQ Comparison	Measure. Obtain the DQ used by the Agency to make the Cloud migration decision and then compare it to the USFCDF DQ, anticipating that the comparison will be in the form of an AoA.
	Metric: The case's DQ is similar to the USFCDF DQ and the answers align with the USFCDF DQ. (conversely, discover no Agency DQ that differed significantly from the USFCDF DQ)

In chapter four, these tests were applied and the results described in the narrative to determine the weight of evidence of each case toward answering question 3b. Again, this can be seen graphically in a Wigmore inference diagram. For example, see the graphic application of these two tests for the VA case study in both Figure 50 and Figure 51 (both diagrams reflect the same Wigmore diagram, but both views are provided for better comprehension).

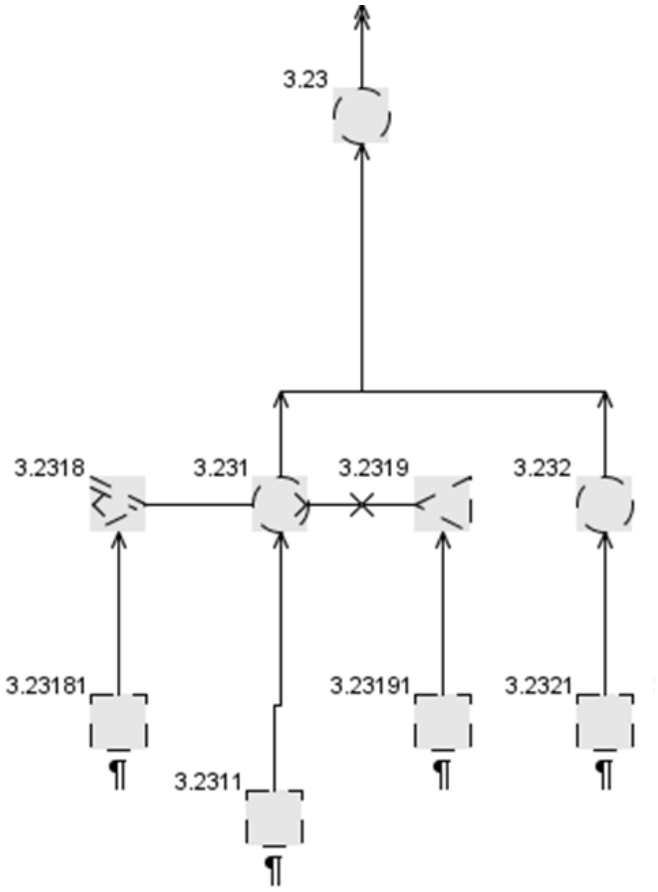


Figure 50 - Graphic of two Q3b tests for VA case (without descriptions)

In both Figure 50 and Figure 51, the top node, #3.23 depicts the evidence toward Q3b from the VA case. The subordinate node, #3.231 represents test 1, which depends on the evidence from node #3.2311. The comparison of the VA DQ and the USFCDF DQ did not match exactly and was noted in node #3.2318. That concern was investigated and countered (node 3.2319). This discrepancy and subsequent adjudication is described in the discussion following Table 46 later in this section. Also note node 3.232. This represents the results of research into how the timing of the potential Cloud migration fit

into the DQ. For all cases, the Cloud migration decision included aspects of timing, typically with the migration to occur as soon as possible.

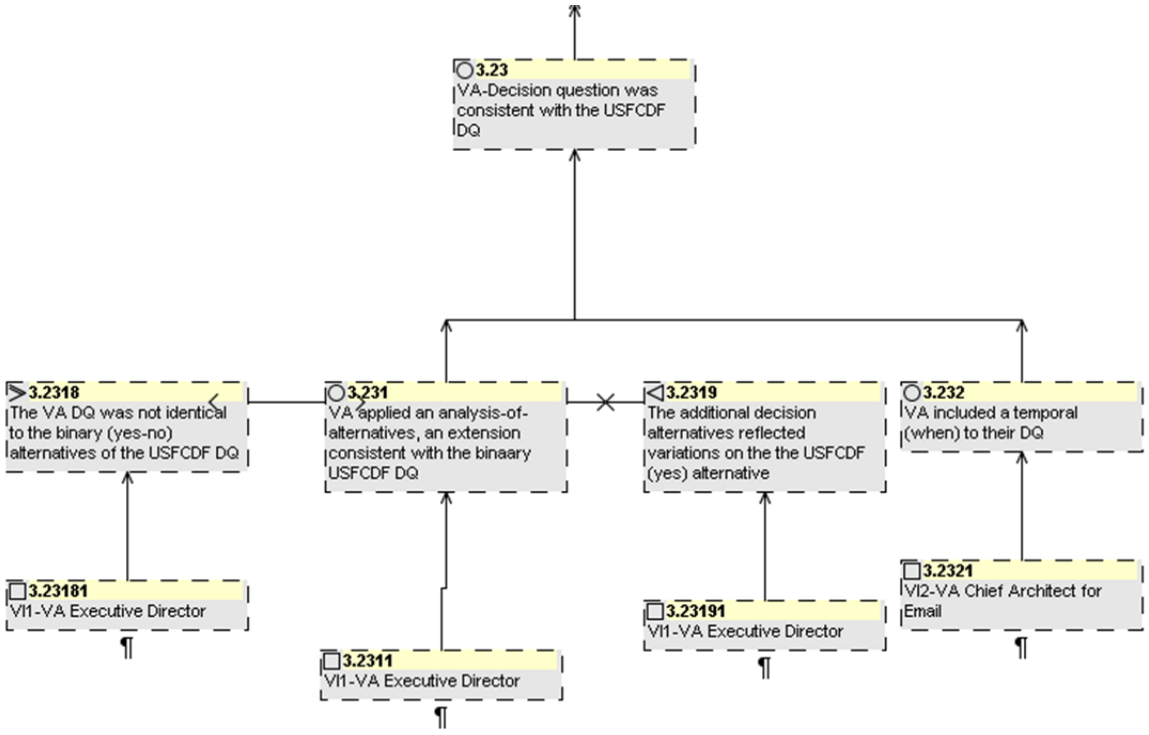


Figure 51- Graphic of two Q3b test for VA case (with descriptions)

With the discussion above providing background, this analysis moves now to combining the Q3b test results from all five cases and synthesizing the results to answer Q3b. Table 46 summarizes the results of the test for Q3b.

Table 46 - Test Results for Question 3b – Is the USFCDF DQ consistent with the needs of the decision maker?

Test Results for Q3b				
Test	**Case**	**Initial Score**	**Further Investigation[19]**	**Adjudicated Result**
1.DQ Comparison	Army	?	More alternatives than yes/no. But aligns	↑
	NSF	?	More alternatives than yes/no. But aligns	↑
	VA	?	More alternatives than yes/no. But aligns.	↑
	GSA	↑	More alternatives than yes/no. But aligns	↑
	USAID	↑		↑
	Synthesis			↑
KEY: ↑ Support ← Detracts ✘ Corroborates ? Doubt n/a Not Accomplished (2= Strong)				

This table follows the same logic and uses the same as Table 36, which was described in the Q1a synthesis previously and will not be overviewed here again.

But, the results of Q3b merit discussion. The test results above indicate that test 1 (comparison of the case DQ and the USFCDF DQ) initially found two cases in support and three in doubt. This doubt was foreshadowed in the earlier discussion about the VA Wigmore diagram (Figure 50 and Figure 51). Further investigation discovered that the doubt in all three cases resulted from the same cause, a DQ with more than two alternatives.

The decision alternatives in those three cases were not just a simple yes/no. Instead, the decision was cast as a comparison of the status quo against several other potential courses of action. This might suggest that the USFCDF DQ was not sufficient for Cloud migration decisions. However, upon further investigation, it was discovered that the

[19] See the respective case study summary in Chapter 4 for elaboration

multiple course of action for those cases mapped nicely onto the binary yes/no choices of the USFCDF DQ as see in Figure 52, using the Army case as an example.

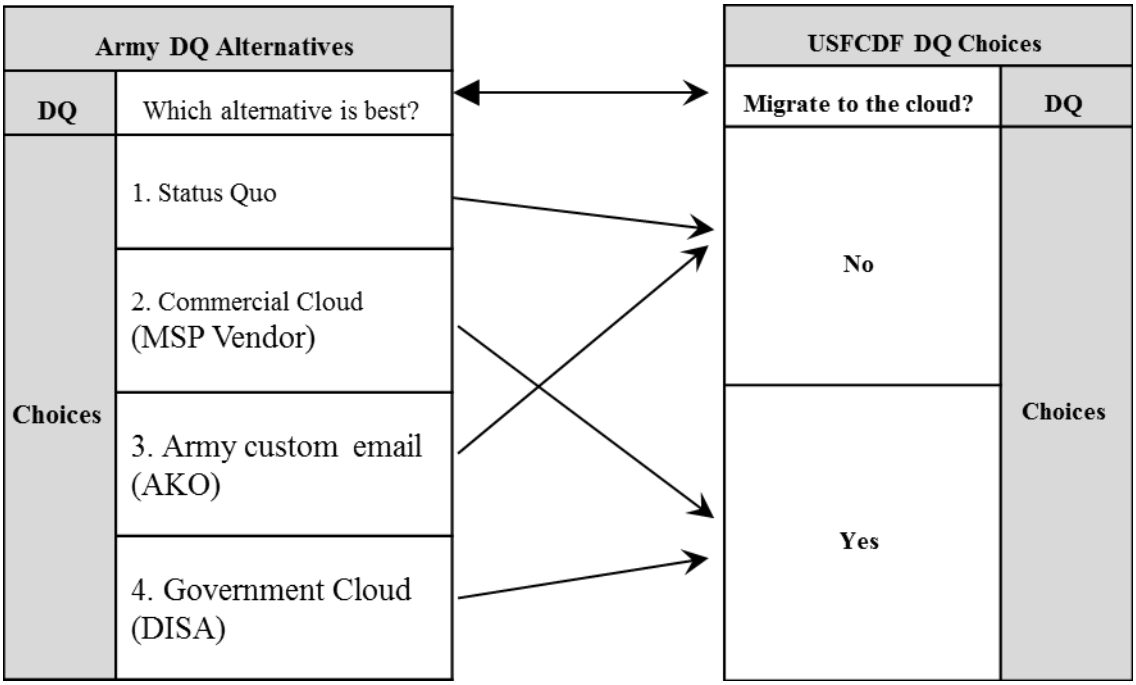


Figure 52 - Comparison of Army DQ to USFCDF DQ

The comparison for the Army case above is very similar to the observations made about the DQ in the NSF and VA cases. The USFCDF DQ aligns with the DQ of all three of the cases. However, as the mapping in Figure 52 suggests, the USFCDF DQ would benefit by recasting itself from a simple binary yes/no DQ to one that allows multiple "yes" and multiple "no" choices.

Together, the support from the five cases supports the conclusion, albeit not strongly because of the DQ rewording needed, that the answer to Q3b is yes, the USFCDF decision question is consistent with the needs of the decision maker.

Q3 – Finding and recommendations

The synthesis from the five case studies strongly supported a "yes" answer to Q3a; the USFCDF decision question is consistent with US Federal guidance and regulations applicable to Cloud migration decisions. This synthesis also supported a "yes" answer to Q3b; the USFCDF decision question is consistent with the needs of the decision maker. Together, the results from Q3a and Q3b moderately support the answer to Q3 that yes, the USFCDF decision question provides value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud.

The synthesis for Q3 also identified the following recommendation related to Q3 that would further enhance the USFCDF:

- Recast the USFCDF DQ from a binary yes/no to an analysis of alternatives (AoA).

Q4 - Is email a well-defined legacy IT system?

It is arguable that the nature of an IT system may affect the efficacy of the USFCDF for migrating the IT system to the Cloud. This research project attempts to generalize the results of this research project beyond email systems to all well-defined legacy IT systems in the Federal Government. This generalization depends on whether email can be considered to represent a well-defined legacy system. This question investigates the

email legacy system so that the results of this research may be generalized to apply to other legacy Federal IT systems.

As noted in Chapter 3, a well-defined legacy system is characterized by its functionality being well understood by potential Software-as-a-Service vendors. This general familiarity eliminates the need for the Federal Agency to embark upon a rigorous project documenting the functional requirements for the legacy IT system. Also, it increases the likelihood that the Cloud marketplace will have multiple vendors capable of providing the functionality. Many back office systems are well-defined, particularly in comparison to new (emerging) systems and organization-unique mission systems. (see Figure 53)

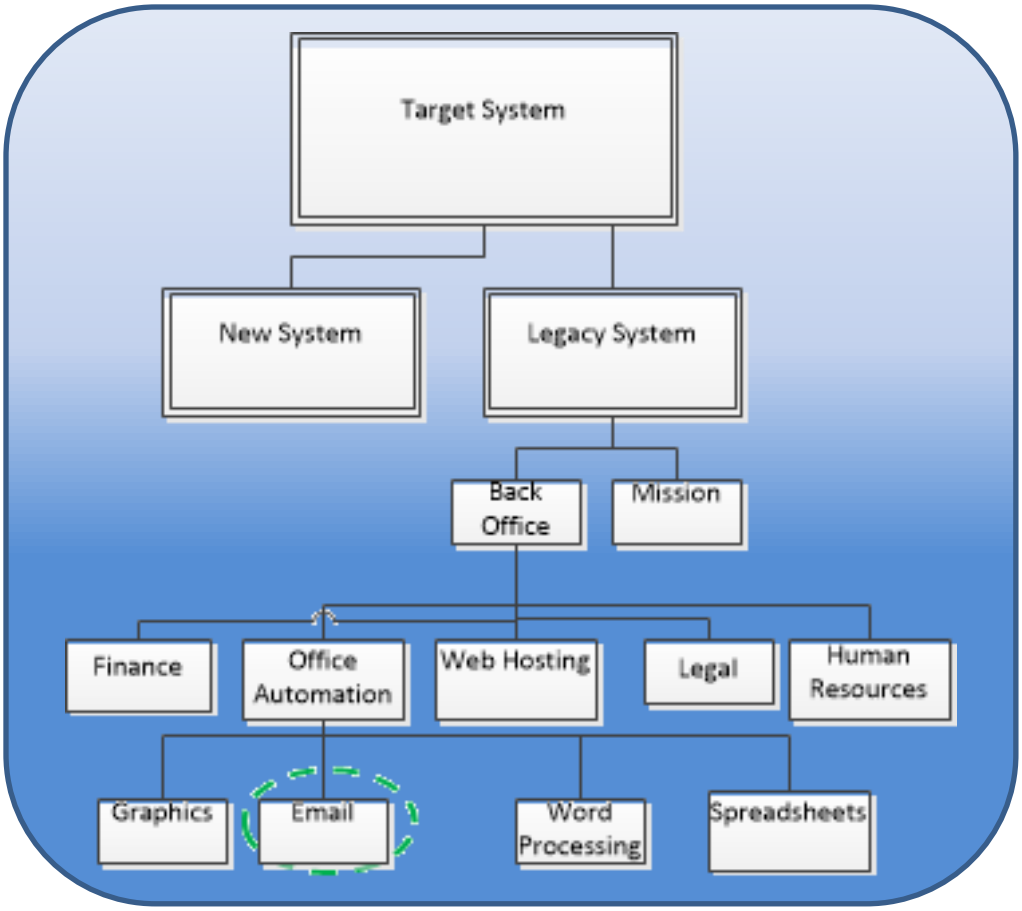


Figure 53 - Email in context of other legacy systems

Q4a & Q4b – Are email systems defined … and is email used across the Federal enterprise?

To answer whether the email is a well-defined system, email systems need to be defined by a small set of legacy commercial projects and email needs to be used across the enterprise indicating common acceptance of its functionality. Specifically this leads to two subquestions:

Q4a. Are email systems in the Federal Government defined by a small set of similar legacy commercial products?

Q4b. Is email used across the Federal enterprise?

Q4a and Q4b are less complex than the previous research questions and are suited to be answered together. To determine whether email can be considered a well-defined system, the researcher attempted to perform two tests across the five cases. This section reviews these two tests and synthesizes the results. The two tests for Q4 are described in Table 46. Each test includes a summary of what was measured and how the measurement would be evaluated.

Table 47 - Tests for Q4

Tests for Question 4	
Test	**Measure & Metric**
1. Commonality	Measure. Identify the email systems used in the five cases. Consolidate the findings
	Metric: Few different legacy vendor systems (average of one vendor per enterprise, five total) across all the cases
2. Span	Measure. Identify the span of usage across each Agency.
	Metric: Email was used across the enterprise

The results of Test 1 are depicted Table 48.

Table 48 – Q4 Test 1 Results

Commonality of Legacy Email Systems	
Case	**Legacy Email System(s)**
1. Army	Microsoft Exchange 2003 using Outlook client Army Knowledge Online (Army custom email)
2. NSF	Microsoft Exchange 2003 using Outlook client and MAC client
3. VA	Microsoft Exchange 2003 using Outlook client

4. GSA	Lotus notes
5. USAID	Microsoft Exchange 2003 using Outlook client
Results	↑↑ Three legacy email systems across all five cases↑↑

Clearly the results of test 1 show that functionality of email was well understood because a few systems defined email for the Federal Agencies. This finding is further validated by noting the Army and VA procurements referenced a legacy vendor product as the basis of their Cloud email requirements to prospective bidders. The functionality of that product defined the functionality required of the Cloud service. Of course, the Cloud service bidders could leverage any product in their Cloud solution as long as the Cloud service provided the required functionality (i.e. they were not locked into using the product that described the functionality). This strongly supports a "yes" to Q4a; email systems in the Federal Government defined by a small set of similar legacy commercial products.

Q4 – Finding and recommendations

The synthesis for Q4b is that all five of the Federal Agencies researched in this report used email strongly support a "yes" answer to Q4a;, email systems in the Federal Government are defined by a small set of similar legacy commercial products.

This synthesis also supported a strong "yes" answer to Q4b; email is used across the Federal enterprise. Together, the results from Q4a and Q4b strongly support the answer to Q4 that yes; email is a well-defined legacy system (suggesting the results of research

on email can be generalized to apply to other well-defined legacy IT systems in the Federal Government).

The synthesis for Q4 also identified the following recommendations related to Q4 that would further enhance the USFCDF:

- Modify USFCDF "government readiness" DF to include an Agency's readiness to document the functional capabilities they require from the Cloud service. Well-defined legacy systems might be considered more ready to migrate than those legacy systems requiring significant requirements definition.

Q5 – Would Cloud migration decision-makers have benefited from prior-knowledge of a validated USFCDF?

While Q4 investigated the generalization of this research project to a large class of legacy systems, this question investigates the potential importance of the research topic to those who would be directly affected by the adoption of a decision framework similar to the USFCDF, Federal IT leaders making decisions on Cloud migration.

To determine whether decision makers would have benefited from prior knowledge of a validated USFCDF, the researcher attempted to perform one test across the five cases using the test described in Table 49. This table summarizes what was measured and how the measurement was evaluated.

Table 49 - Tests for Q5

Test for Question 5	
Test	**Measure & Metric**
1. Indicators	Measure. Identify indications about the benefit the Agency would perceive from the USFCDF and the likelihood of the Agency adopting the USFCDF

	Metric: Preponderance of observations indicate benefit and likelihood

The results of Test 1 are depicted in Table 50.

Table 50 - Test results for Q5

Would IT leaders have benefited from a USFCDF? Were they likely to have adopted it?			
Case	**Indicator**	**B**	**L**
1. Army	Decision questioned later for lack of validated documentation	↑	?
	Testimony "I think it [validated USFCDF] would have been great value"	↑	↑
	Testimony "Oh, absolutely. Without question".	↑	↑
	Started process "trying to make sense of how to move forward"	↑	?
2. NSF	Sought out early adopters to leverage their insights	↑	↑
	Waited on GSA for acquisition vehicle and FedRAMP	↑	↑
	Conservative culture, risk adverse	↑	↑
3. VA	Sought out best practices from early adopters and Garner Consulting	↑	↑
	Decision later reversed by other non-IT stakeholders	↑	?
	Decision questioned later for lack of validated documentation	↑	?
4. GSA	Applied prior Cloud experience to craft their own decision framework	↑	?
	Spearheaded FedRAMP, indicating support for Government-wide actions	↑	↑
	Spearheaded Cloud acquisition contract vehicle, indicating support	↑	↑
5. USAID	Applied prior Cloud experience to craft their own decision framework	↑	?
	Sought out best practices from early adopters	↑	?
	Made Cloud migration decision informally	←	←
Results		↑↑	↑
Key: ↑ Support ← Detracts X Corroborates ? Doubt (B)enefit (L)ikelihood (2= Strong)			

The results of test 1 strongly show that decision makers would have perceived benefit from the USFCDF had they adopted it. Furthermore it is likely that they would have adopted the USFCDF even without it being required by Federal regulation. Several cases

noted that, should the USG require them to use a framework like the USFCDF, such guidance would likely guarantee adoption.

Q5 – Finding and recommendations

The synthesis for Q5 moderately supports a conclusion that Cloud migration decision-makers would benefit from prior knowledge of a validated USFCDF.

The synthesis for Q4 also identified the following recommendations related to Q5 that would further enhance the USFCDF:

- Incorporate the USFCDF into Federal guidance on IT capital investments. The likelihood of adoption, and therefore the realization of the benefits of the USFCDF, would increase as Agencies seek to comply with Federal guidance.

Varying Replication Logic

Rationale for varying two characteristics of the cases

This research project hypothesizes "*The US Federal Cloud Decision Framework (USFCDF) provides value to Federal IT decision makers in determining whether a well-defined legacy IT system should migrate to the Cloud."* To investigate the hypotheses, this research project followed the case study methodology recommended by the leading authority in case study methodology, Robert Yin (see Chapter 3). Yin recommends consistency among the cases and only varying characteristics of the case for specific predetermined reasons. For this research project, the researcher deliberately ensured the cases varied in two ways to support the generalization of the hypothesis. Specifically, the case selection criteria in Chapter 3 required that the cases vary two characteristics::

1. Size of the IT system migrating to Cloud. This study attempts to identify whether the study can be generalized to both large and small migrations. Therefore this research will include a case or partial case for a large as well as a small migration.
2. Nature of Federal Agency mission. This study attempts to identify whether the study can be generalized across all Federal Agencies, including both civil and national security agencies.

The case study characteristics – both replicative (non-varying) and varying – are depicted in Table 51.

Table 51 –Replicative (non-varying) and varying characteristics of cases researched

Case		Replicative Logic Constants				Planned Variations	
Agency	Full/ Partial	Cloud Migration Decision	Legacy IT System	Delivery Model (SaaS)	Relatable to Theory	System Size	Agency Type[20]
Army	Full	✓	✓	✓	✓	Large	DoD
NSF	Full	✓	✓	✓	✓	Modest	Non-DoD
VA	Full	✓	✓	✓	✓	Large	Non-DoD
GSA	Partial	✓	✓	✓	✓	Modest	Non-DoD
USAID	Partial	✓	✓	✓	✓	Modest	Non-DoD

This variation in case characteristics drove two additional research questions:

V1: Does the size of the IT system migrating to the Cloud affect the answers to the primary research questions (Q1 – Q5)?

[20] The only military agency migrating email at the time of this research was DoD. Other DoD organizations waited to learn the verdict of Army's initiative before they migrated to Cloud email. After Army email demonstrated success, the DoD CIO pre-empted further decisions at the remaining DoD organizations by issuing a memo requiring all DoD organizations to migrate to DISA's Cloud email. Therefore, this research project only included Army, but the approach Army used was endorsed across DoD, justifying the single Army case to represent the planned variation for national security mission.

V2: Does the nature of the Federal Agency affect the answers to the primary research questions (Q1 – Q5)?

The anticipated result, which supports the hypothesis, is that the answer to both V1 and V2 are "no," the size of the IT system and the nature of the Federal Agency do not alter the answers to Q1 – Q5.

V1 and V2 – Finding and recommendations

The tests for V1 & V2 were structured identically.

For V1 (size of legacy IT system), each subquestion was tested by comparing the results of the cases with large legacy IT systems (Army and VA) to the results of the cases with modest legacy IT systems (NSF, GSA, and USAID). For each comparison, the unweighted adjudicated results were compared so that the results benefited from further investigation but excluded extra weight given to full cases. The test for V1 indicated no significant differences between cases with large IT systems and those with modest IT systems.

For V2 (nature of Federal Agency), each subquestion was tested by comparing the results of the case with a mission related to national security (Army) to the results of the cases with missions other than national security (NSF, VA, GSA, and USAID). As with the test for V1, the unweighted adjudicated results were compared so that the results benefited from further investigation but excluded extra weight given to full cases. The test for V2 indicated no significant differences between the Army and the other cases. There was a minor difference in the strength of support for Army's yes answer to Q2b The Army indicated stronger support than non-Army cases for one test (see Table 42),

but this was only a difference in level of support and this difference was not discovered in the other test for Q2b or in tests for other research questions.

The answers to V1 and V2 are no ,there are no significant differences in the research results caused by either the size of the legacy IT migrating or the nature of the mission of the Federal Agency.

Synthesis of Other Observations

This section serves to synthesize other observations discovered during the case that not found to be tied directly to the five research questions. Table 52 provides an index to these observations and noted which observations had surfaced in multiple cases.

Table 52 - Other key observations related to Federal Cloud migration decisions

Other Observations[21]			
Case		**Observation**	**R**
1. Army	1	The decisions process and associated decision gates	✓
	2	Decision documentation	✓
	3	Cost and efficiency	✓
	4	Federal guidance and Cloud migration	✓
	5	Acceptance of NIST Cloud definitions	
2. NSF	1	The decisions process and associated decision gates	✓
	2	Decision documentation	✓
	3	Dependence on First Movers	✓
	4	Federal guidance and Cloud migration	✓
3. VA	1	The decisions process and associated decision gates	✓
	2	Decision documentation	✓
	3	Funding (CapEx and OpEx)	
	4	Federal guidance and Cloud migration	✓
	5	Shifting Responsibility to Cloud Vendors	
4. GSA	1	Prior Cloud success encourages subsequent Cloud migration	✓
	2	Adopting Public Cloud	✓
5. USAID	1	Prior Cloud success encourages subsequent Cloud migration	✓
	2	Security is Relative	
	3	Adopting Public Cloud	✓
	4	The decisions process and associated decision gates	✓
	5	Decision documentation	✓
	6	Cost and efficiency	✓
Key: (R)ecurring – Observed more than once			

While Chapter 4 discussed these in relation to each case, it is worth highlighting some synthesized findings from these observations:

1. The decisions process and associated decision gates. The Cloud migration is not a single decision, but rather a series of decisions gates that build on each other[22]. Therefore the USFCDF should be structured to accommodate the decision

[21] See the specific case summary in Chapter 4 for elaboration.

22 This research project investigated the decision gate that resulted in the Cloud implementation.

evolution. For example, the USFCDF should account for an early gate that emphasized security, which subsequently narrows the remaining alternatives in later gates to only consider secure Cloud options. This happened for the Army case study. After ensuring all their alternatives had met security regulations, they omitted Security as a further consideration.

2. Cost and efficiency. Although cost savings is promoted as a key reason to migrate to Cloud, and Federal IT leaders show cost savings in their rationale after the fact, these cases suggest decisions to migrate to Cloud were not based primarily on cost savings.
3. Federal Guidance and Cloud migration. Many agencies mentioned the Federal CIO's support for Cloud as a factor supporting their Agency's Cloud initiatives. Leadership is important and codifying Cloud guidance does affect Cloud migration.
4. Dependence on first movers. All five cases indicated that they explore Cloud migrations at other organizations (including universities, firms, and other Agencies) prior to making their own Cloud migration decision. This indicates that the USFCDF should be examined to discover how it might be applied to enable the Federal Government to capture best practices of prior Cloud migrations. This observation also suggests implicitly that the USFCDF readiness dimension should include a consideration for risk. Insights collected from successful prior migrations could provide insight to lower the risk of future Cloud migrations. Another aspect of this observation is that some Federal Agencies are

more risk adverse or more financially constrained, and may defer a Cloud migration until the risks or costs are reduced. For example, NSF elected to defer their implementation until FedRAMP, the Cloud security assessment and accreditation, was put in place. Overall, this observations indicates that Federal IT leaders are influenced by activities outside their Agency and the USFCDF should reflect that observation.

5. Public Cloud. Two Agencies included public Cloud as an alternative to their legacy IT system in their Cloud migration decision. Subsequently, they both implemented public Cloud. This indicates that the USFCDF can support more decisions involving public Cloud as well as decisions involving Cloud hosted by another government agency or Cloud vendors hosting only other Government-only customers.
6. Funding (CapEx & OpEx). Although scoring only one observation, this topic surfaced in many conversations. CapEx and OpEx are mentioned without explanation in Kundra's definition of the USFCDF efficiency decision factor. Capital expenses (CapEx) refer to the upfront investment required for new IT systems. Operating expenses (OpEx) refer to ongoing sustainment costs. Legacy email systems required OpEx with occasional spikes of CapEx for upgrades. Cloud services are almost exclusively paid through OpEx. For these reasons, IT leaders may see significant benefit in IT services funded through OpEx instead of hard-to-obtain CapEx.

7. Security is relative. USAID noted that far from considering Cloud less secure, Cloud would actually provide them a more secure service than their own email system. It appears that Cloud security is relative to current security and Agency security requirements. This observation is a myth buster, countering the prevalent belief that Cloud is less secure than traditional IT systems.
8. DF labels and definitions. During the case interviews, the researcher encountered multiple incidents where the Federal IT leaders misinterpreted the meaning of a decision factor. Although this misinterpretation was clarified to ensure the quality of the research, the incidents suggested the USFCDF could be improved by relabeling some DFs and reviewing the definitions of all DFs for consistency and clarity.

Findings of Multi-Case Study

This results of this research project strongly support the conclusion (the ultimate probandum) that The US Federal Cloud Decision Framework (USFCDF) provides value to Federal IT decision makers in determining whether a well-defined legacy IT system should migrate to the Cloud.

Furthermore, each of the sub-hypotheses (the pentultimate probanda) are supported, with particular strength of support noted for the first sub-hypothesis.

Sub-hypothesis 1:

The USFCDF decision factors[23] provide value to the Federal IT decision maker.

Sub-hypothesis 2:

[23] Underlines represent the essence of the particular sub-hypothesis or subsub-hypothesis.

The USFCDF decision structure provides value to the Federal IT decision maker.

Sub-hypothesis 3:

The USFCDF decision question is consistent with the needs of decision maker.

This is clearly apparent from the consolidated results of the research questions and their linkage to this conclusion.

Consolidated answers to research questions

The results of this multi-case study are summarized in Table 53, which is organized to align with this project's research questions. For each research question and subquestion the table presents the answer and the strength of support this answer provides to the conclusion.

Table 53 - Synthesized answers to research questions

Research Question	Answer	Strength
1. Do the USFCDF decision factors provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?	Yes	↑↑
a. Are all USFCDF decision factors necessary?	Yes	↑↑
b. Is the set of USFCDF decision factors sufficient?	Yes	↑↑
2. Does the USFCDF decision structure provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?	Yes	↑
a. Does a decision structure (in general) provide value?	Yes	↑↑
b. Is the Value-Readiness paradigm of the USFCDF decision structure useful for marshalling decision factors	Yes	↑
3. Does the USFCDF decision question provide value to Federal IT leaders deciding whether a legacy IT system should migrate to the Cloud?	Yes	↑
a. Is the USFCDF decision question consistent with US Federal guidance and regulations applicable to Cloud migration decisions?	Yes	↑↑
b . *Is the USFCDF decision question consistent with the needs of the decision maker?*	Yes	↑
4. Is email a well-defined legacy IT system?	Yes	↑↑
a. Are email systems in the Federal Government defined by a small set of similar legacy commercial products?	Yes	↑↑
b. Is email used across the Federal enterprise?	Yes	↑↑
5. Would Cloud migration decision-makers have benefited from prior-knowledge of a validated USFCDF?	Yes	↑
KEY: ↑↑ Strongly Supported ↑ Supported ? Doubt		

As can be seen from the results, the answer to all the research questions and subquestions was positive. Furthermore, the evidence for each answer provided either support or strong support for the conclusion. None of the answers suggested doubt.

Supporting the Conclusion

The answers to the first three research questions directly support the research conclusion. This can be seen graphically by examining the Wigmore diagram[24] in Figure 54

[24] See Appendix E for details on how to view these diagrams in Araucaria, the Wigmore diagramming tool.

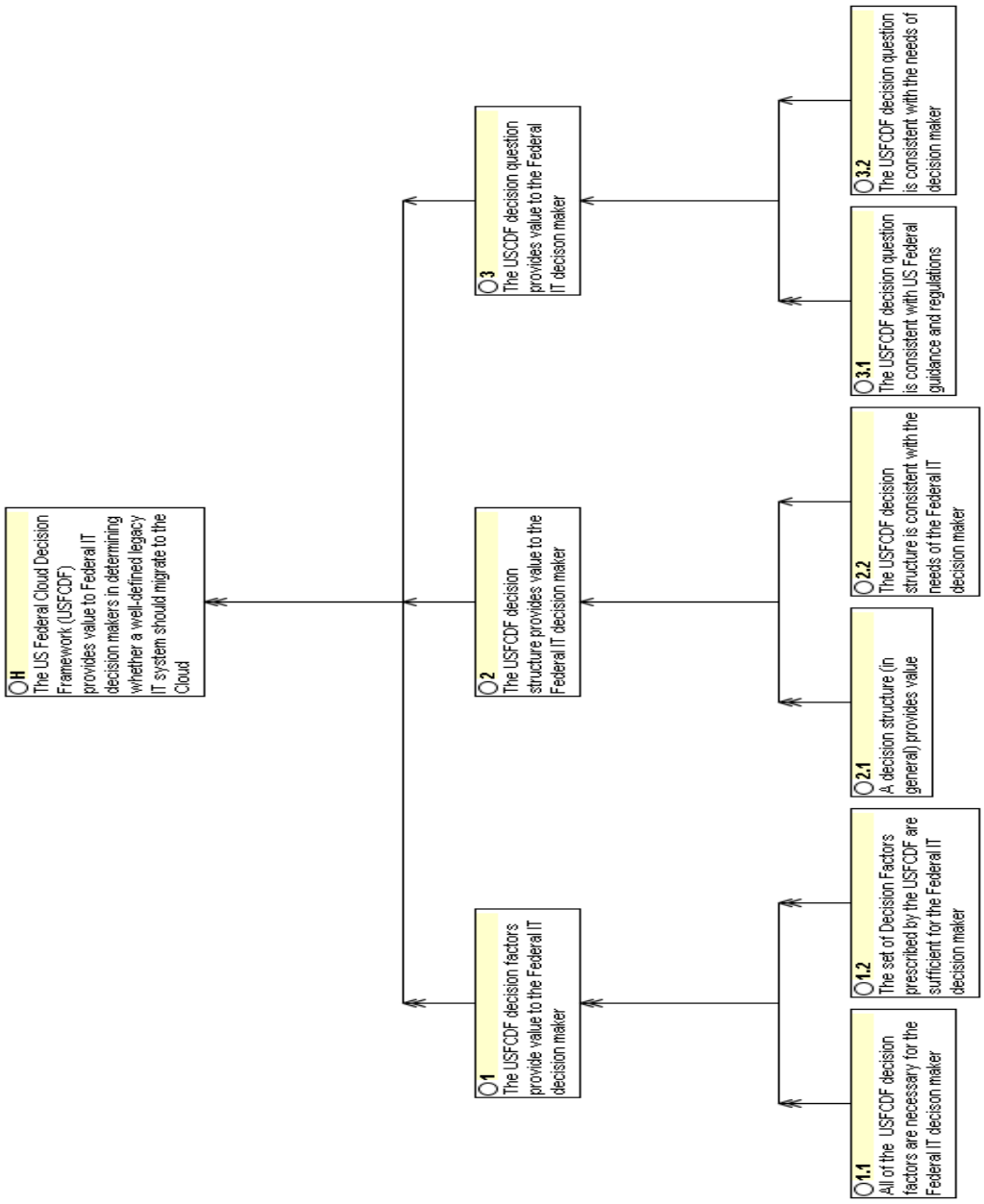


Figure 54 - Wigmore diagram linking two levels of sub-hypotheses to the hypothesis

Note the IDs in each box corresponding to the hypothesis, the three sub-hypothesis, and the supporting subsub-hypotheses. The arrows indicate the force of support, the vertical

direction represents positive support and the arrow head representing either strong (double arrowhead) or moderate (single arrow) .

The hypothesis is further supported by the results of question 5, which can be seen graphically by examining the Wigmore diagram in Figure 55.

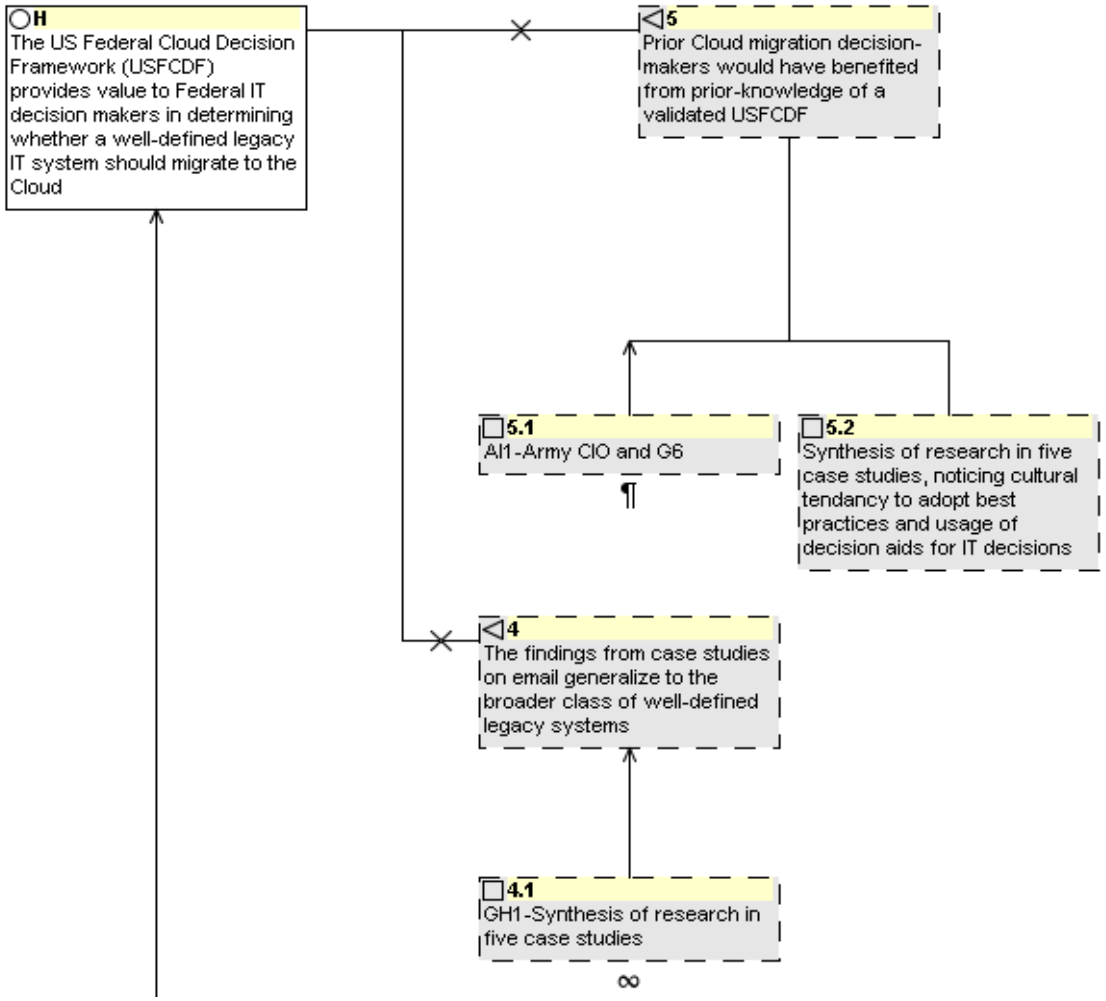


Figure 55 - Wigmore diagram showing corroboration

In the previous diagram, box 5 depicts the corroborative support from case study analysis as well as a testimony from a senior IT leader who made the decision for the largest cloud migration in the Federal Government to date (Army email).

Box 4 depicts how the answer to question 4 supports the generalization of these research results to migration decisions for all well-defined legacy systems in the Federal Government.

Increasing the USFCDF's value for Federal IT decision makers

This research project concluded that the USFCDF provides value to Federal IT decision makers in determining whether a well-defined legacy IT system should migrate to the Cloud. The research also discovered insights for increasing that value. Those recommendations are listed below.

- ✓ Modify the set of existing DFs to include consideration for "alignment of resources with implementation." In other words, consider the availability (readiness) of funds for the migration effort in addition to the benefit (value) of the eventual efficiency from a successful migration to Cloud
- ✓ Align the documentation used for the decision (the USFCDF documentation) with that required for subsequent reporting. Such government requires reporting all expected investment costs as well as the eventual cost savings. This may entail expanding the scope of the USFCDF readiness dimension to include considerations for the cost of the migration itself.

- ✓ Review the overarching definitions of efficiency and readiness so they are not (as is the case now for efficiency) defined primarily by the decision factors they contain. In particular, identify readiness closer with migration, to avoid Agencies creating DS categories such as "operations" that contain DFs relating to both value and readiness.
- ✓ Recast the USFCDF DQ from a binary yes/no to an analysis of alternatives (AoA) that characterized the "no" choice as the status quo and expands the "yes" to include multiple alternatives to the status quo.
- ✓ Review the remainder of the USFCDF documentation to ensure it is consistent with recasting the DQ as an AoA.
- ✓ The definition of the USFCDF government readiness should include a consideration on the ability of the Agency to define the functional capabilities they require from the Cloud service. Well-defined legacy systems might be considered more ready to migrate than those legacy systems requiring significant requirements definition.

5. CONCLUSION

Theoretical and practical implications

The US Federal Government owns over 12,000 IT systems. The Agency responsible for each system must spend resources (manpower and funds) to develop, operate, modify, and refresh the system. Collectively, this effort costs $80B a year. Cloud offers US Federal Agencies the means to reduce costs while improving their capabilities.

Some Agencies have put a toe in the water and have migrated a few legacy IT systems to the Cloud. But progress has been slow. The decisions migrations seldom leverage the analysis and insights from previous decisions. Each new decision carries with it the risk of overlooking a small but unseen factor. The problem, to date, has been that US Federal Agencies lack a common, validated decision framework for deciding whether a legacy IT system should migrate to the Cloud.

In 2010, the US Federal CIO (Vivek Kundra) proposed a Cloud decision framework referred to in this paper as the US Federal Cloud Decision Framework (USFCDF). But, Kundra departed the Federal Government for other opportunities before his decision framework was tested and validated.

This research project investigated the decisions by five agencies to migrate their email to the Cloud. Each Agency independently developed its own decision framework and process for their Cloud migration decision. This research project found the commonality among the decisions by using the USFCDF as a common reference model. The

USFCDF served as a Rosetta stone for translating the components of multiple Cloud migration decisions into one common perspective. The conclusion was that the USFCDF, if adopted for a Cloud migration decision, will provide value to the decision maker. The research also identified ways the USFCDF could be enhanced to provide even greater value to those decision makers.

The practical implication of these results is a validation of the USFCDF and rationale for its adoption as the general framework for all Cloud migration decisions. The framework has the flexibility to remain relevant, applicable, and beneficial for variations typical across Agencies and their associated candidates for migration to the Cloud. It provides a framework to help an Agency collect meaningful data on the factors important for the decision. It also organizes these factors into a decision structure that promotes the right discussions about the value of the potential migration and the readiness of the vendors and the Agency to migrate the system. The framework can frame the decision question in a fashion that can then be incorporated into the formal justification required of IT actions in the Federal Government. The USFCDF, once adopted as the standard decision framework across the Federal Government, can become the organizing construct to capture data and lessons learned from Cloud migrations. This body of knowledge can further improve IT decisions while reducing the risk of future decisions. The USFCDF, once validated and adopted across the US Federal Government, will also help IT leaders describe and defend their Cloud migration decision to stakeholders within and external to their Federal Agency. Together, the prospect of better decisions and less risk should result in more and smarter use of Cloud services to reduce IT costs and improve an

agency's ability to accomplish its mission. This has the potential to significantly reduce the $80B spent each year on IT in the Federal Government.

The results of this investigation also further the body of knowledge about Cloud and the Federal Government. Prior studies have primarily explored only the risks of moving to the Cloud and this research was accomplished primarily through opinion surveys of IT leaders. This research project explored both the value and the risks of Cloud migration. It also suggests the application of a value-readiness paradigm for technology decisions, extending the concept of the Technology Acceptance Model from adoption decisions at the individual user level to adoption decisions at the enterprise level.

Limitations and recommendations for future research

Although this research project investigated five cases of Cloud migration decisions (three full case studies and two partial case studies), the decisions had occurred in the past and without employing the USFCDF. This suggests that a case study in real time employing the USFCDF might provide additional insights into this research problem. This research project focused on a specific Cloud delivery model, a few of the Cloud deployment models, a single (albeit extremely large and diverse) organization, and a single type of legacy systems (well defined IT systems like email). Figure 1 depicts the applicable span of this problem area, and the areas outside the scope of the project. Research into these other areas would likely expand our knowledge on the general problem area about Cloud decisions.

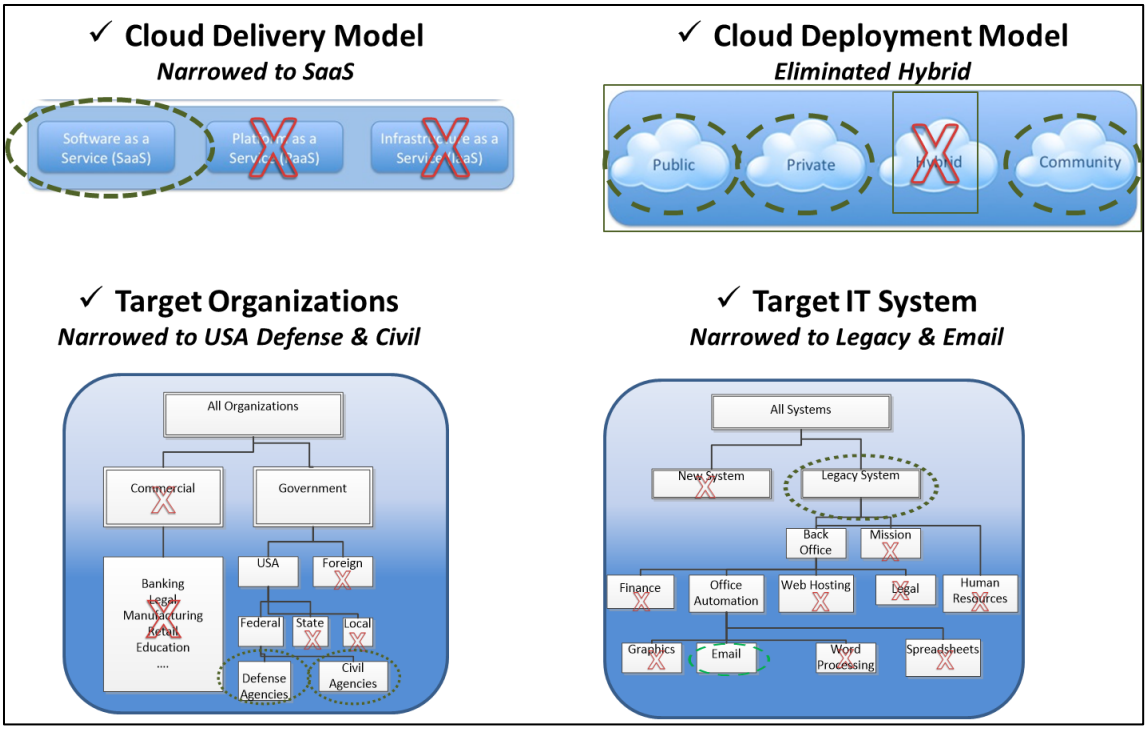


Figure 56 - Limitations of results and potential research areas (denoted by X symbols)

Finally, this research identified enhancements to the USFCDF that hypothetically should further increase the framework's potential value to Federal IT leaders. Research validating these enhancements would further increase our understanding of Cloud migration decision frameworks and result in a better decision framework overall.

Closing

Former US CIO Kundra saw the potential benefits of Cloud for Federal Agencies. He coined "Cloud First" across the Federal Government and proposed the USFCDF for Cloud migration decisions. This research project strongly validated the USFCDF and suggested opportunities for increasing its value further. This results of this research project also validated the need for a common decision framework for Cloud migration

across the Federal Government. This should be rallying cry for US Government leaders to formally adopt the USFCDF so that better Cloud decisions can improve US Agencies' performances and reduce what they spend to achieve that performance.

APPENDIX A: CASE STUDY 1 (ARMY) BACKGROUND

Introduction

This appendix provides additional background on the case study research into the US Army's decision to migrate their legacy email systems to a cloud-based email service. For this appendix, the terms US Army, Army, and USA are synonymous and interchangeable.

This case researched the 2010 decision by the Department of the Army to migrate their legacy email systems to a DISA cloud service initially named Army Enterprise Email (AEE) and subsequently renamed Defense Enterprise Email (DEE). AEE used Software as a Service (SaaS) for their cloud delivery model (see Chapter 2) and Community Cloud as their deployment model (see Chapter 2). Lieutenant General Jeffrey Sorenson, Army CIO and G6, led the decision making process and served as senior decision maker.

The investigations for this case followed the methodology described in Chapter 3. The Army's champions for this case study research were Lt General Susan S. Lawrence, successor to LTG Sorenson as Army CIO and G6, and her deputy, Mr. Michael E Krieger. This case benefited from multiple investigative sources including: LTG Sorenson, Lieutenant Colonel Peter Barclay (Project Team Lead), internal Army documentation surrounding the decision, and numerous external publications surrounding the decision.

The Federal Organization – US Army

The US Army is largest of the four Services within the Department of Defense. Most readers are probably already familiar with this Federal Organization and Army's mission -- "The Army exists to serve the American people, protect enduring national interests, and fulfill the Nation's military responsibilities. Specifically, the Army mission is to provide to combatant commanders the forces and capabilities necessary to execute the National Security, National Defense, and National Military Strategies. Army forces provide the capability-by threat, force, or occupation-to promptly gain, sustain, and exploit comprehensive control over land, resources, and people."(Army 2005) As such, the Army is an extremely large enterprise, consisting of 1.125 million military members authorized for 2012, increasing to over 1.5 million email users when counting civil service and contractors.(Burrelli 2012) Although much of the organization is located in garrison at fixed sites (The Institutional Army) many of the members belong to Army Service Component Commands (The Operational Army - see Figure 57) that deploys to and operates from austere locations boasting limited network bandwidth and reliability. The Army's size, mission, and diverse operational footprint make it arguably the most challenging organization to adopt a Cloud solution for its internal communications – email.

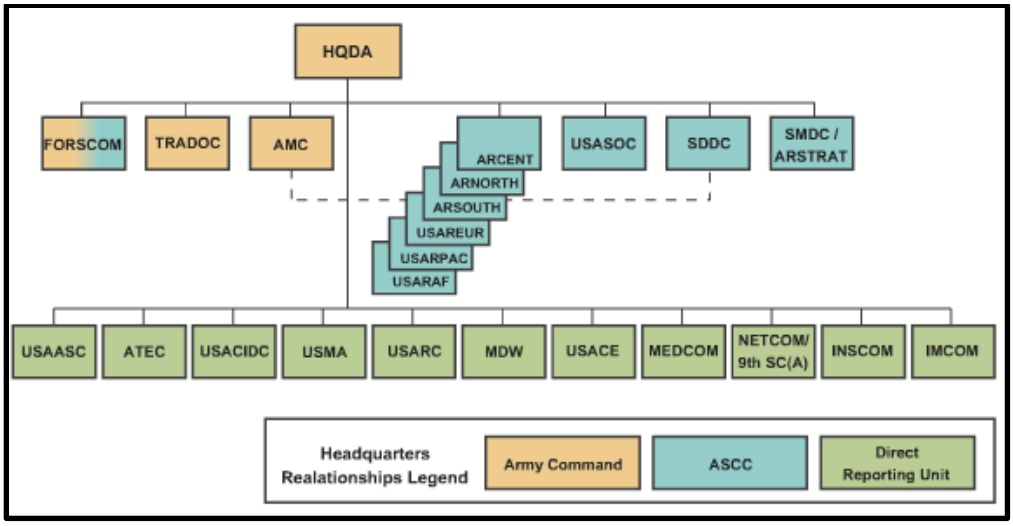


Figure 57 - Department of Army Organization (with Relationship to CIO/G6 added)(Army 2012)

The Legacy IT System

Prior to adopting Cloud, the Army hosted two email capabilities: 1) Microsoft Exchange 2003 hosted at 18 enclaves across the Army enterprise, and 2) Army Knowledge Online (AKO), a web-based email solution.(Army February 2012).

In contrast to other military Services, such as the Department of Navy's Navy-Marine Corps Intranet (NMCI), the Army initially adopted an approach to IT and email that empowered the local commander to provide services that best suited the soldiers under their command – "centralized policy by design with decentralized execution."(Army February 2012) In the Army's 2012 report to Congress, the Army explains their situation as the embarked on Enterprise Email.

> Between 1995 and 2007, Army networks developed in a decentralized fashion (centralized policy by design with decentralized execution). Installations were responsible for determining the best method to deliver capabilities to their tenant

organizations, and each major organization determined the best method to provide coherent, integrated solutions to its subordinate components, often spread across the globe. … In 2008, the Army determined that it still had at least 18 different network enclaves in existence with redundant Microsoft Exchange Email systems across the globe. The large number of disparate and redundant networks, along with the high number of servers and personnel required to maintain them over the life cycle of the systems, resulted in high costs and significant operational inefficiencies across the Army. Most Army installations hosted their own Microsoft Exchange servers and employed the necessary support staff. …

This segmentation of service produced a number of inefficiencies and operational risks for the Army, such as:

1. Lack of calendar-sharing across organizations
2. Lack of delegation privileges to users in other organizations
3. Inefficiencies as Soldiers and Civilians transfer between duty stations
4. Duplicate email services deployed throughout the Army
5. Duplicate email administration responsibilities
6. Underutilized hardware
7. Potential security vulnerabilities due to multiple disparate authentication mechanisms, including in some cases, username/password
8. Lack of Continuity of Operations (COOP) capability

9. Non-compliance with statutory and regulatory requirements to journal specific email messages (Army February 2012)

The roots of enterprise email were laid by the Service's enterprise portals. In the late 1990's, the Army and the Air Force each developed a portal as a common front end for users to access their Service's IT capabilities. For the Air Force, this initiative was one of thirteen that fell under the "One Air Force, One Network" set of IT Initiatives headed by this researcher. For the Army, this initiative started as an experimental project by the General Officer Management Office but was then transferred to COL Robert Coxe as part of a larger portal effort named Army Knowledge Online (AKO).(Coxe 2000)

One of the capabilities provided by AKO was email. This email was unique in that, unlike the Army's Exchange Email, a user's email address remained unchanged throughout reassignments, deployments, and even retirement from the Army. AKO was transformational in that Army members – from Generals to Privates as well as Army Civilians came to personally recognize the power of an enterprise-wide, user-oriented application. AKO employed robust technology for the time -- an architecture built around Sun products. However, AKO email lacked an ability to interact with local networks for authentication. "the lack of adequate functionality and lack of integration with local networks and network operations hindered its widespread adoption as the Army's single email service provider…" (Army February 2012). Furthermore, the architecture of AKO eventually created a bottle neck that hampered performance when scaled (see Figure 58).

The Army was hosting two email systems – MS Exchange at separate installations globally and AKO which could not handle growing demands for security and scalability. Neither system seemed capable of meeting the Army's growing needs for more email capability.

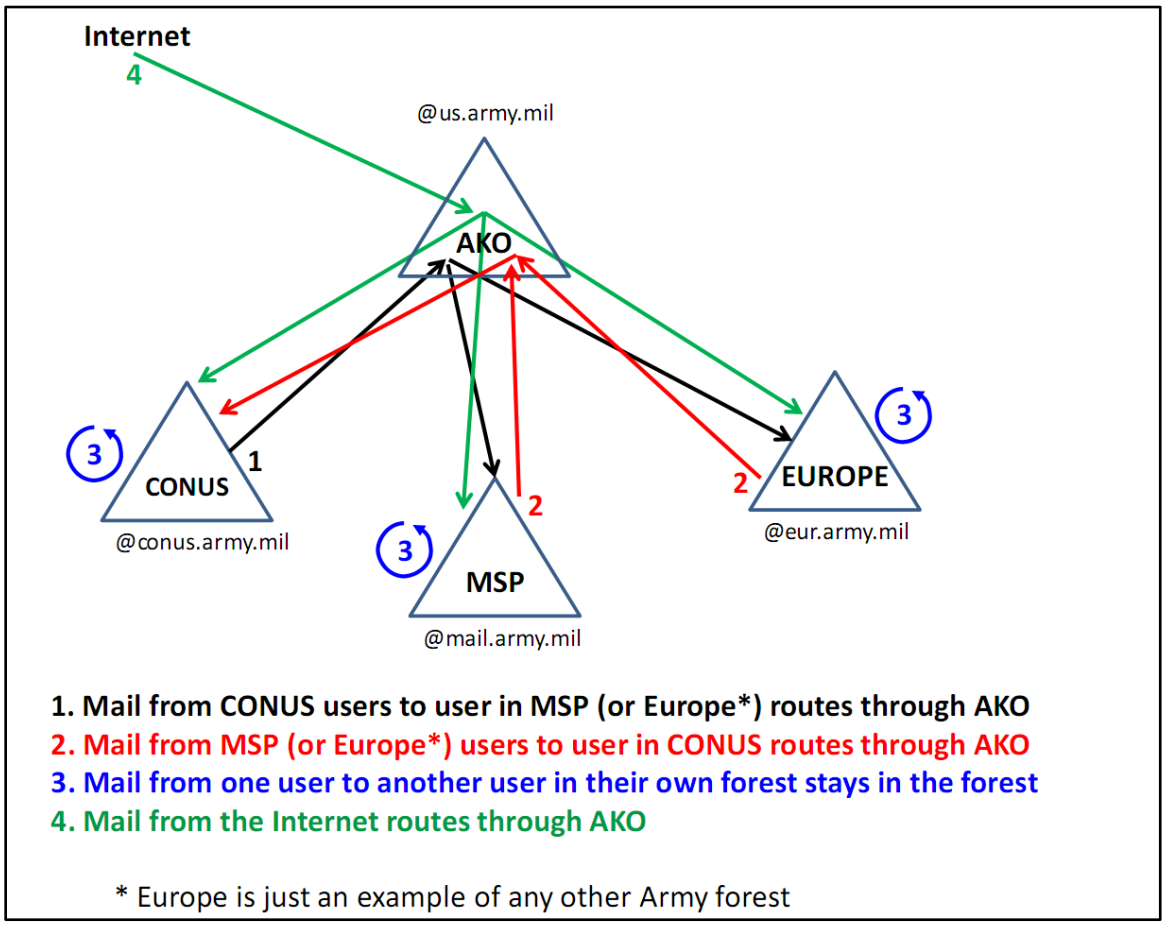


Figure 58 - Depiction Email Routing Flow (Barclay 2010)

The Cloud Decision

The decision to migrate to Cloud was led by Lieutenant General Jeffery A. Sorenson, who held the position of Army Chief Information Officer/G6 at the time(Barclay 2012). Formal approval was obtained through the Army's governance process that included

several decision review committees. The Army applied a decision framework based on an analysis of competing courses of action (COAs)(Burrelli 2012). In other words, the decision wasn't simply a "yes/no" regarding migration to cloud. Rather, LTG Sorenson presented the current (legacy) system as of the competing courses of action titled "Status Quo," which competed against other cloud and non-cloud alternatives.

Decision Makers

The primary decision maker for Army's migration to Cloud was LTG Sorenson. General Sorenson was the Army's senior signals officer, the career field that evolved to include oversight for information technology. In addition, LTG Sorenson served as the Army Chief Information Officer in accordance with the Clinger-Cohen act. The military leader often serves multiple roles or fill multiple positions simultaneously– an arrangement referred to as "dual hatted."

Perhaps the most influential person shaping the structure of the decision an action officer - LTC Peter Barclay. LTC Barclay was also a career signals officer. His formal position was Director, Army CIO/G-6 Advanced Technology Directorate, an organization that tiered up to LTG Sorenson. His primary responsibility was to lead the Army Enterprise Email effort. In the spring of 2012, LTC Barclay was recognized for his role in Enterprise Email by being selected as one of the 100 government and industry leaders who have gone above and beyond their daily responsibilities and have made a difference in the way technology has transformed their agency or accelerated their agency's mission. (FCW 2012)

Decision Process

The decision to migrate the Army's legacy IT systems to cloud occurred over time in a series of decisions.

The initial decision was to have the Defense Information Systems Agency (DISA) provide an email cloud service to Army and other Defense users.(Sorenson 2012). However, the Army felt that, at the time, DISA was not adequately prepared to provide this service in a timely, full-featured, and cost-effective manner.

In 2008, the Army decided to explore migration to a commercial cloud provider. The Army leveraged Gartner as a resource and established a working group create the first draft of a decision framework and associated decision factors (Army 2008). This initial work led to a decision by the Army to embark upon a commercial cloud provider and the first major action in such an acquisition was that the Army released a Request for Information (RFI) soliciting industry's insights and capabilities for hosting the Army email in a cloud(Olson 2009). This RFI summarized the decision as follows: "The Army seeks to consolidate 850,000+ NIPRNet and 100,000+ SIPRNet business email user accounts on servers currently distributed across Army installations to a centrally managed email system for each network. In addition to the business user accounts, the Army would like to separately migrate an additional 1.2+ million retiree and family member accounts from distributed organizations to a separate centrally managed email system with lower performance requirements outside of the official business environment. …Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and

released with minimal management effort or service provider interaction. This cloud model promotes availability and is comprised of five key characteristics, three delivery models, and four deployment models." At this point, the Army had decided it would migrate both of its legacy email systems to cloud; that the provider would be commercial – but could host in a commercial facility or government facility; that the deployment model was Private Cloud, the delivery model Software as a Service. This RFI also listed "constraints" that generally mapped to the USFCDF category of "Readiness."

However, to procure a cloud service from commercial sources the Army had to follow rules and procedures laid out in DoD acquisition guidance such as DoD Directive 5000.1, "The Defense Acquisition System."(AT&L 2003) The challenges of acquiring IT in the Federal Government are documented extensively(Wynne 2010). One of these challenges is that in most cases, Congressional funding for an IT initiative is usually limited to a specific time period, which is usually a given year. If the funds are not committed by the end of that time period, the funding is lost. With end of fiscal year 2010 approaching, the Army decided to resurrect the decision to use DISA as a cloud provider. Instead of creating a new decision framework for evaluating DISA as a cloud provider, the Army retained its earlier decision framework but incrementally compared DISA to a commercial provider. The Army had already determined that the commercial cloud provider was a better option than the legacy system, and this modified decision framework found that DISA was a better option than a commercial provider.(Burrelli 2012) LTG Sorenson made this decision, briefed it to the Senior Budget, Requirements, and Program (BRP) Group (see Figure 59 –Army Decision Organizations – Budget, Requirements, and Program Board (PRP)(Army Force Management School 2010)

Figure 59) and received approval to proceed. Soon thereafter, LTG Sorenson directed DISA to begin activity to stand up Enterprise Email for the Army.

As mentioned earlier, the decision to migrate to the DISA Cloud occurred through a series of decision gates. For example, LTG Sorenson briefed the Army Senior Budget, Requirements, and Budget (BRP) Board on September 24, 2010 to revalidate a previous decision to migrate to Cloud. The Secretary of the Army chairs the BRP and the Chief of Staff of the Army is the BRP Vice Chair. At this meeting, these two senior Army leaders re-approved the decision to migrate to Cloud.

Subsequently, the Army recertified this decision (i.e. decided that the decision to migrate remained correct) several times. For example, even after the Army had already migrated thousands of users to the Cloud, Congress directed the Army restructure the effort as an

acquisition program for the Secretary of the Army to certify that "the selected approach for moving forward is in the best technical and financial interest of the Army…"(Army February 2012)

The Under Secretary of the Army included its planning for Enterprise Email in the Army Business Transformation Plan submitted to the Congress on October 1, 2010. In December 2010, The Army released an Execution Order to all commands to migrate to Enterprise Email. The Secretary of Defense included Army information technology efficiencies from consolidation of email servers and data centers in his January 2011 report on efficiency initiatives. The October 2010 information was updated slightly and communicated again in the March 1, 2011 Department of the Army 2011 Annual Report on Business Transformation, Providing Readiness at Best Value.(Congress 2011)

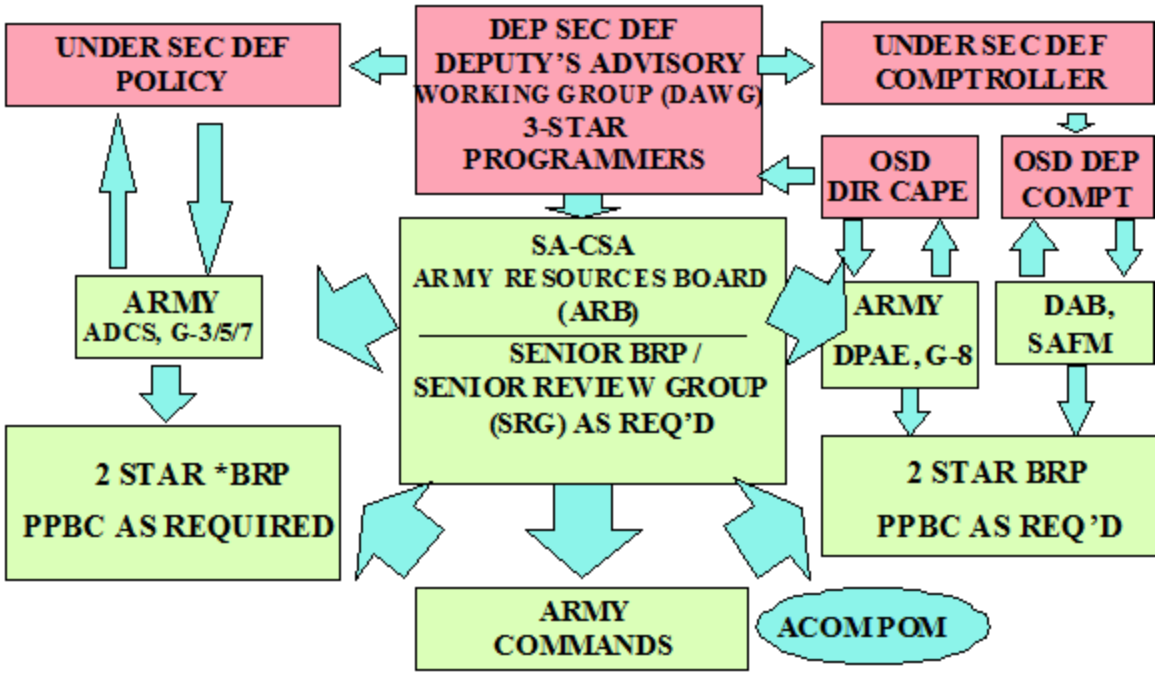


Figure 59 –Army Decision Organizations – Budget, Requirements, and Program Board (PRP)(Army Force Management School 2010)

However, Congress expressed concern about the Army decision. When the President signed the 2012 National Defense Authorization Act (NDAA) in December 2011, the Act contained language directing the Army to explain its decision to migrate legacy email to a DISA cloud.(Congress 2011) Furthermore, the Army was directed to stop spending on AEE until they complied with guidance in the NDAA and answered specific questions posed in the NDAA. The Army report back to Congress was to include "A certification by the Secretary of the Army that the selected approach for moving forward is in the best technical and financial interests of the Army and provides for the maximum amount of competition possible in accordance with section 2302(3)(D) of Title 10, United States

Code." Congress also directed that the "Secretary of the Army shall designate the effort to consolidate its enterprise email services a formal acquisition program with the Army acquisition executive as the milestone decision authority. The Secretary of the Army may not delegate the authority under this subsection." (Congress 2011). In February 2012, the Army reported back to Congress. In their report, the Army summarized their decision to migrate legacy IT systems to Cloud. What had begun as a project to explore alternatives to the aging legacy IT systems had evolved into a high-interest acquisition monitored closely by Congress.(Army February 2012)

The AEE DF's, DS, and DQ, are the focus of this research. Yet the evolution of the AEE decision provides insight into the Army's evolving rationale for the decision. For example, although unstated in the 2012 report to Congress, the difficulty in acquiring IT -- email in this case -- as an Army acquisition program caused the Army to again consider DISA as a cloud provider. The subtly here is that the Army was seeking a Private (Army) Cloud for email built and maintained by a contractor. But, DoD acquisition regulations drove a process that precluded timely transition to Cloud. In particular, funding for Cloud email might expire at the end of the fiscal year, and it became apparent that an acquisition process for a Private Cloud through a contractor would take too long – the funds might be lost. But, funds could be transferred to DISA before they expired. DISA would build a Cloud for email that could serve all DoD – a Community Cloud. The Army's decision to adopt Community Cloud over Private Cloud as the Cloud deployment model was driven primarily by expediency.

Another observation is that, although Army cited cost savings as an important factor in their decision to migrate to cloud, at the time of their early decisions, they had collected little data about the costs and savings as compared to the financial analysis provided to Congress in 2012.

The evolution of the decision and associated decision factors presented the researcher with the unanticipated challenge of determining which decision in the sequence of decisions should be analyzed for this research project. Should the final decision – for example the 2012 report to Congress – be considered the definitive decision because it was the most recent and contained the most detailed support? Or, was the report to Congress simply an exercise to justify a decision already made? In the latter case, which of the preceding decision announcements should be considered the definitive case? The definitive decision was selected based on the logic that the decision that resulted in action initiating the migration should be considered primary. Therefore, the September 2010 decision briefing to the BRP is the definitive decision for this case study. This session initiated activities to stand up AEE. Documents and sessions prior to that meeting informed the definitive decision. Documents and sessions subsequent to that meeting could be considered validation events that provide greater insight into the original decision. For example, in January 2012 the Office of the Deputy Army Auditor General concluded that LTG Sorenson's estimates for costs for DISA cloud were understated and that the costs of legacy AKO email were overstated.(Army 2012) Although not explicitly asked about which decision he considered definitive, LTG Sorenson supported the researcher's conclusion by describing the BRP as the time the

Army made the decision to migrate to cloud. Also of interest, LTG Sorenson indicated that the Army gained additional insight after the decision about the importance of factors for migrating to cloud. Therefore this research captures the Army decision framework and decision factors at the time of the BRP but also incorporates insights subsequently gained about this framework and decision factors from revisits to the decision as well as form lessons learned by the Army as it implemented the decision.

Conduct of the Case Study

This case study was conducted in accordance with the case study protocol described in Chapter 3. The researched included the following investigational sources:

- LTG Jeffry Sorenson, former G6 and Chief Information Officer of the Army. LTG Sorenson was the decision maker and also facilitated the ratification of his decision through various Army and DoD review boards. Researcher interviewed LTG Sorenson twice (initial and follow-up), and also exchanged information though emails.
- LTC Peter Barclay, Project Officer for Army Enterprise Email. LTC Barclay facilitated the decision process. This included development of the evolving decision framework, integration of advisors such as Gartner, and preparation for LTG Sorenson's review boards. Researcher met with LTC Barclay twice (initial and follow-up), exchanged emails, and also talked by phone.
- Multiple source documents. Researcher obtained and reviewed minutes from initial meetings as well as the briefing for the formal decision ratification

presented by LTG Sorenson and ratified by the Army leadership. Many of these documents were classified "For Official Use Only (FOUO)" and therefore could not be quoted in this paper without classifying the overall dissertation. However, the researcher quoted documents not FOUO and also compared statements by the interviewers against the FOUO documents to validate the interviewers statements. Together, these investigational sources met the triangulation requisites of Chapter Three and supported the findings of this research project.

APPENDIX B: CASE STUDY 2 (NSF) BACKGROUND

Introduction

This chapter discusses the research into the National Science Foundation's decision in August of 2010 to migrate their legacy email systems to a cloud-based email service. This chapter leads with a concise summary of the researcher's findings from this case. That's followed by an overview of the case to include background on the organization, the legacy IT system, the cloud decision, and the conduct of the case study. Finally, each investigation composing the case study is related along with the results of this case study investigation.

This case researches the August 2010 decision by the National Science Foundation to migrate their legacy email systems to cloud. As of spring 2013, NSF had not selected their Cloud Service Provider as this subsequent decision was likely to take the form of a procurement decision, about which information is considered highly sensitive. The senior decision-maker, Dorothy Aronson, head of IT Operations and Special Assistant to the Director, led the decision making process. Her team selected Software as a Service (SaaS) for their cloud delivery model (Chapter 2) and either Public Cloud or Private Cloud as their deployment model, eliminating the Hybrid and Community Cloud deployment models (see Chapter 2).

The investigations for this case followed the methodology described in Chapter 2. NSF's champion for this research investigation was the NSF CIO, Amy Northcutt. Investigative

sources for the case included Amy, Nick Ipiotis, Infrastructure Service Branch Chief, and a third senior IT leader who requested anonymity (subsequently referred to as Interviewee 3. Some NSF documentation – particularly working papers surrounding the decision also informed this case study investigation.

The Federal Organization – NSF

Congress established the NSF in 1950 with a mission that continues to shape NSF's activities and culture today: *To promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes(Congress 1950)* The eight primary functions of the NSF are:

> (1) to develop and encourage the pursuit of a national policy for the promotion of basic research and education in the sciences;
>
> (2)to initiate and support basic scientific research in the mathematical, physical, medical, biological, engineering, and other sciences, by making contracts or other arrangements (including grants, loans, and other forms of assistance) for the conduct of such basic scientific research and to appraise the impact of research upon industrial development and upon the general welfare;
>
> (3)at the request of the Secretary of Defense, to initiate and support specific scientific research activities in connection with matters relating to the national defense by making contracts or other arrangements (including grants, loans, and other forms of assistance)for the conduct of such scientific research;
>
> (4) to award, as provided in section, 10, scholarships and graduate fellowships in the mathematical, physical, medical, biological, engineering, and other sciences;

(5) to foster the interchange of scientific information among scientists in the United States and foreign countries;

(6) to evaluate scientific research programs undertaken by agencies of the Federal Government, and to correlate the Foundation's scientific research programs with those undertaken by individuals and by public and private research groups;

(7) to establish such special commissions as the Board may from time to time deem necessary for the purposes of this Act; and

(8) to maintain a register of scientific and technical personnel and in other ways provide a central clearinghouse for information covering all scientific and technical personnel in the United States, including its Territories and possessions.

Today, according to NSF's current Strategic Plan, NSF accomplishes their mission – and their corresponding eight functions – by managing portfolios of research and education using a competitive merit review aligned with national priorities.(NSF 2011) This same strategic plan notes that to be effective with their mission, NSF "promotes a culture of excellence that encourages diversity, creativity, and initiative." As NSF noted of themselves, they operates from "bottoms up" and eschews a "top down" process (NSF 2013-1). This cultural aspect of NSF is highlighted because it was found to be a significant factor in NSF's Cloud decision process.

NSF has a budget of $7B (NSF 2013-1) and provides 20% of the research funding for basic research at America's colleges and universities. In some research fields, NSF provides direct grants and is the only significant source of research funding. NSF has a workforce of 2,100, making it significantly smaller than other federal organizations such

as the US Army in terms of personnel (vice budget). Of this 2,100, approximately 10% are research scientists on temporary duty from their research institutions.

NSF's organization includes a National Science Board, Directors Staff, seven Directorates, and two Support Offices. (see Figure 60) The seven Directorates resemble lines of business – or operational divisions – in a commercial firm. The Directorates manage the research activities and investments central to the mission of NSF. The Director's staff functions advise the Director. The two Support Offices provide internal support for the seven Directorates as well as for NSF overall. IT management resides within one of these two Support Offices -- The Office of Information & Resource Management (OIRM). The NSF CIO, Amy Northcutt, is a co-lead for this office. One of the three Divisions within OIRM is the Division of Information Systems (DIS), led by Dorothy Aronson. Under DIS is the Infrastructure Services Branch, let by Nick Ipiotis and focusing on enterprise infrastructure management, to include issues related to Cloud.

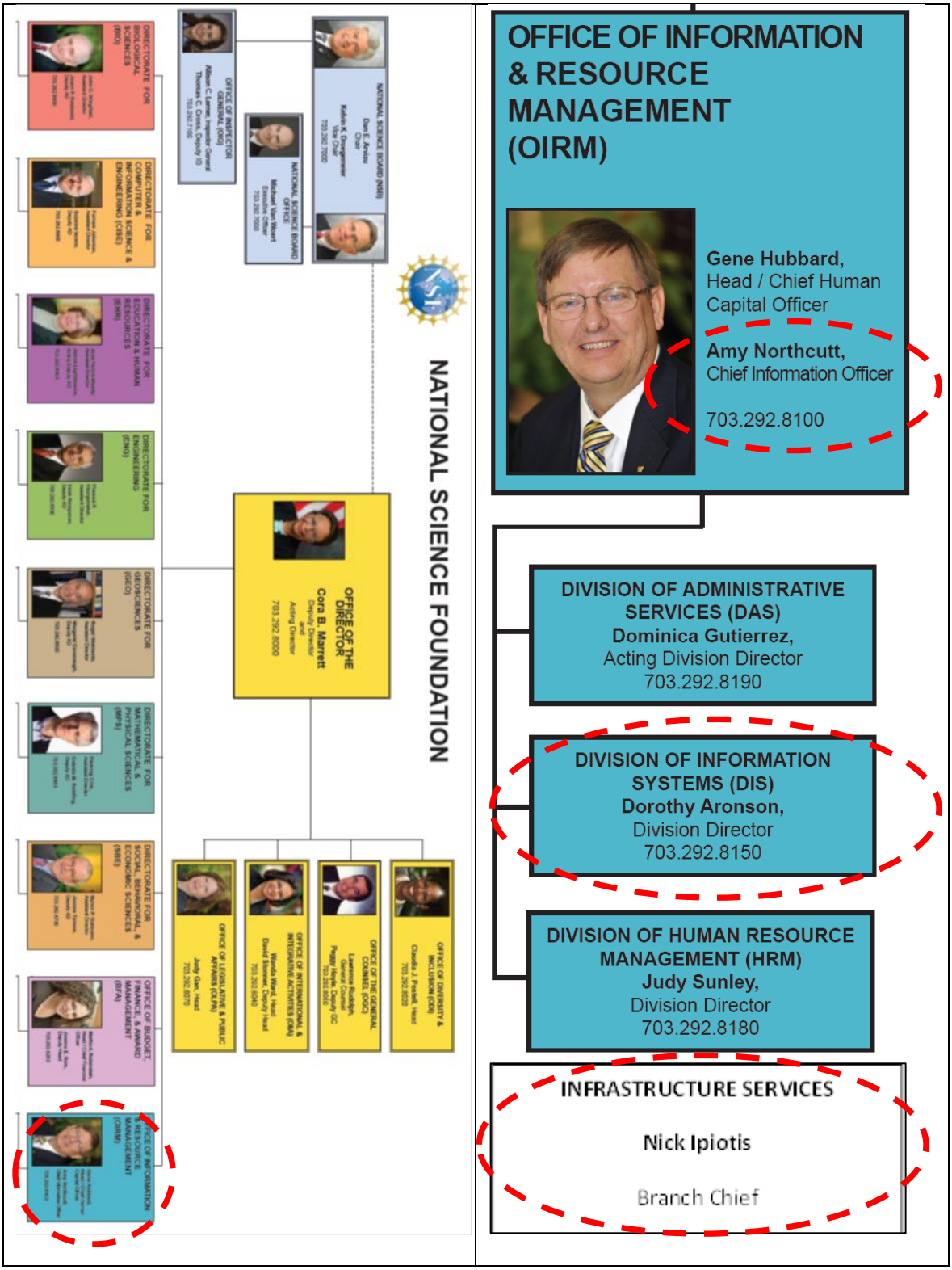


Figure 60 - NSF Organization Highlighting Key Decision Organizations

The Legacy IT System

NSF provided email service through local (decentralized) instantiations of Microsoft Exchange 2003. As of summer 2010, Microsoft Exchange 2007 was the predominant Microsoft email server and Microsoft Exchange was the current release for traditional email services.(Ipiotis 2012) In other words, NSF's back-end email technology significantly lagged that used by most other Federal organizations and available commercially.

Exchange 2003 provided NSF a baseline of email, along with calendar, contacts, and tasks. This service was tightly coupled with Blackberry support hosted by NSF as well as single sign-on and secure remote access.(Ipiotis 2010) This legacy system supported 2,500 user accounts. Account holders used one of two types of NSF-supplied user devices to access their legacy email back end -- MACs or PC-type computers (desktops computers and laptops).

These end-user devices supported one or more user-level software clients:

1) Outlook 2007, suitable for PC-type computers running MS Windows

2) Entourage, suitable for MAC computers, and

3) Outlook Web Access (OWA), accessible by any computer with a web browser.

The MACs operated under Apple operating systems and the PC's operated under Microsoft operating systems. Because the legacy email system (Exchange 2003) was a Microsoft product, and itself a somewhat dated version of the email server, MAC users only had access to a limited set of features that provided primarily basic email and calendaring capability. PC users, on the other hand, benefited from a much richer feature

set as their email client (MS Outlook) was more closely coupled with the MS Exchange 2003 back end.(Ipiotis 2012)

The decentralized implementation of NSF email fit the culture of NSF described earlier. But as the Federal pressure for data center consolidation grew, the NSF IT leadership gained leverage to consider NSF enterprise-wide approaches to services such as email. Furthermore, the former head of NSF's IT Division observed the success of transforming a decentralized payroll system into a centralized payroll system hosted nearby in Ashburn, VA, but – significantly – outside of a NSF facility. This favorable experience with enterprise consolidation, combined with guidance such as the pending Federal Data Center Consolidation Initiative[25], created the condition for NSF to explore an enterprise approach to NSF email.(Leader 2012)

The Cloud Decision

The decision to migrate to Cloud was led by Dorothy Aronson, Director of Information Systems, who held the position of Special Assistant to the IT Division Chief at the time (Northcutt 2012). Formal approval was obtained through the NSF's governance process that included several decision review committees. NSF applied a decision framework based on an analysis of competing options. In other words, the decision wasn't simply a "yes/no" regarding migration to cloud. Rather, NSF considered the presented the current (legacy) system one of the competing options referred to as "Current NSF Email," which then competed against the four other cloud and non-cloud alternatives. (See Table 54)

[25] See Chapter Two for a summary of the Federal Data Center Consolidation Initiative (FDCCI)

Current NSF Email (Exchange 2003)	Google (Gmail)	MS Cloud "BPOS" (Exchange 2007)	MS Federated Cloud (Exchange 2007)	MS Cloud "365" (Exchange 2010)
Host Location: Local	Cloud	Cloud	Dedicated (34 wks)	Cloud
Services: Baseline (email, calendar, contacts, tasks)	Baseline plus IM without tasks	Baseline plus IM	Baseline plus IM	Baseline plus IM
Clients: Outlook 2007 Entourage OWA	Outlook 2007 Gmail	Outlook 2007+ Entourage OWA Outlook 2011 MacMail/iCal (not supported)	Outlook 2007+ Entourage OWA Outlook 2011 MacMail/iCal (not supported)	Outlook 2007+ Entourage OWA Outlook 2011 MacMail/iCal
State of Readiness: Production	Production	Production	Production	Beta (March '11)
Pilot status: N/A	DIS pilot complete	DIS pilot underway	Pilot not available	Available for pilot
Blackberry Support: Hosted at NSF	Hosted at NSF	Cloud	Included	Cloud
Single Sign-on: Yes	No – Hosted at NSF	No	Yes	Anticipated
Secure Remote Access: Yes	Yes	No	Yes	Anticipated
Cost: High	Low	Low	High	Low

Table 54 - NSF Email Options

The status quo option was described earlier in this chapter in the section titled *The Legacy IT System* and won't be repeated here. Option 2 was Google Gmail. Most readers are familiar with Gmail from personal use. Of importance to NSF was that Gmail provided the same baseline services as the status quo except that it lacked the capability to manage "tasks," Gmail provided instant messaging/chat, which the status quo lacked. Gmail provides access through a browser, but also serves as the back end for local email clients such as Outlook. Gmail was ready at the time of the decision. (NSF Dec 2010) NSF noted that Gmail lacked support for NSF's mobile device, the BlackBerry. Gmail

also lacked single sign-on authentication, which required a separate authentication system hosted at NSF.

The third option was Microsoft Business Productivity Online Suite (BPOS), Microsoft's first foray at providing traditional desktop applications from the Cloud as SaaS. MS BPOS is based on MS Exchange 2007. As expected, BPOS provided the same capabilities as the baseline, while also providing instant messaging/chat. MS BPOS supported Outlook 2007, Entourage, and OWA as user interfaces, but not Outlook 2011 or MacMail/iCal for the Mac systems. Furthermore, BPOS was weak on security, lacking single sign-on authentication and secure remote access.

NSF's fourth option was MS Federated Cloud using Exchange 2007. This solution was in reality a hosted/dedicated solution that upgraded NSF form Exchange 2003 to Exchange 2007, and linked the multiple instances of Exchange into one federated solution. Because this was a hosted solution, it provided both single sign-on and secure remote access, but required a considerable capital outlay.

The final option for NSF was MS Cloud "365." This was Microsoft's follow-on to BPOS. 365 would be available shortly (March 2011) and addressed the shortcomings NSF had identified in BPOS – 365 supported Mac clients and was anticipated to provide security through single sign-on and secure remote access.

Decision Makers

The primary decision maker for NSF's migration to Cloud was Dorothy Aronson.(Ipiotis 2012; Northcutt 2012) Dorothy was one of the most senior IT leaders in the organization. NSF divided IT management into two parts generally referred to as Government Business

Applications and Commercial Off the Shelf (COTS) Productivity Systems, which included NSF email.(Leader 2012) In addition, Dorothy served as Special Assistant to the IT Division Director[26]. A Federal leader often serves multiple roles or fill multiple positions simultaneously– an arrangement referred to as "dual hatted."

The most person who shaped the decision for Aronson was Nick Ipiotis.(Northcutt 2012) Nick helped identify decision factors and data around those factors. At the time, Ipiotis was an IT Computer Specialist working for a federal contractor and responsible as lead for the project. A significant benefit of this option is that it combined all email addresses across NSF – allowing access and look-up. Ipiotis describes his background as having "more than twenty two years of experience with Information Technology systems, including fourteen years of experience with design and implementation of computer networks including local and wide area networks design and implementation, office automation applications including e-mail and directory services, and network and application management systems." (Ipiotis 2013)

The Director of NSF appointed Amy as Northcutt Chief Information Officer (CIO) of NSF in January 2012. The NSF CIO is responsible for NSF's information technology investments, governance, policy, and planning. (NSF 2013-3). In August 2010, Northcutt was not instrumental in the NSF Cloud Decision, but did observe the decision process from her position as Deputy General Counsel of NSF. (Northcutt 2012)

Decision Process

[26] Subsequently, Aronson was promoted to the permanent position of Division Director

Although NSF decided to move to Cloud in August 2010, the project began in Spring 2010 as a study about Hosting Alternatives -- "what we [NSF] should do next with the hosting of our infrastructure." (Ipiotis 2012). Several events coincided to prompt the study that initially had little to do with Cloud itself. For example, NSF's lease for its building (and hence its IT hosting site) was coming due and the Federal Agency contemplated moving. Another factor was that some of the IT infrastructure was obsolete and required a refresh. For example, NSF operated Microsoft Exchange 2003 on aged servers from the same era. Finally, NSF activity had "grown dramatically," driving a need for more capable computing. The study evolved over the summer, and concluded that some applications, particularly NSF-unique applications were not suitable for Cloud hosting but that others, particularly Email and with its associated functions such as calendars and contacts, appeared to be a candidate for migrating to Cloud. During this research process, NSF investigated other organizations that had either adopted Cloud for email – such as Berkley Laboratories, or were developing acquisition approaches that NSF could leverage – such as the General Services Administration (GSA). (Northcutt 2012) The summer 2010 effort also developed the decision framework and decision factors that structured NSF's decision. Finally, this analysis effort narrowed the potential Cloud providers (firms) from an initial set of four (Microsoft, Google, Cisco, and IBM), to two finalist firms – Google and Microsoft.(Ipiotis 2012)

The August 2010 decision to migrate NSF email to Cloud did not produce any formal decision documents. (Leader 2012). Rather, Aronson reviewed the results of the report with her team and concluded that NSF should move email to Cloud. As noted in Table

54, NSF had identified three alternatives for Cloud – Google, MS BPOS, and MS 365. The decision to move to Cloud resulted in guidance for next steps -- to analyze the Cloud alternatives and select the best cloud option among those three alternatives. The decision in August 2010 to migrate to cloud may be seen as fundamental in retrospect, but at the time was seen more as just another step in multi-step project to modernize NSF hosting. The August 2010 decision set the stage for subsequent decisions about the shape and specifics of NSF's Cloud solution.

In November 2010 – after the Cloud decision -- NSF began to gather data for two leading options – Google Gmail and MS BPOS. NSF experimented and researched Google Gmail and embarked on a full pilot of MS BPOS. By December 2010 it was apparent that MS 365 was eclipsing MS BPOS, so NSF did not feel BPOS merited further exploration and the pilot shifted to MS 365. Although the results of the analysis indicated a clear winner, NSF has not formally announced their final Cloud choice because that information was sensitive.

Conduct of the Case Study (NSF)

This case study was conducted in accordance with the case study protocol described in Chapter 3. The researched included the following investigational sources:

- Amy Northcutt, Deputy General Counsel of NSF from 2011-2011; and also Acting Office Head of Information and Resource Management; appointed CIO of NSF in January 2012. From her positions, Northcutt participated in, advised, and observed the Agency's decisions. She was interviewed for this research in March 2012, having been appointed CIO several months earlier. Northcutt's multiple

positions and her senior position as CIO, enabled her to provide valuable insights into the decision and the decision process.

- Nick Ipiotis, IT Computer Specialist and Project Lead for NSF Infrastructure Study. Ipiotis developed the NSF decision categories, identified the NSF options (including Cloud), provided the analysis of alternatives, and presented the results to Aronson, the decision maker.
- Source Three, was a senior IT leader at NSF who was extremely familiar with the decision from its early stages, through the August 2010 decision, and with subsequent perspective through the interview in April 2012. This person requested anonymity and non-attribution. The researcher maintains files and transcript of this interview for research integrity. The pronoun "he" or "she" may be occasionally used to reference Source Three but such usage does not imply gender or other personally indefinable information.
- Multiple source documents. Researcher obtained and reviewed documents relating to the hosting alternatives (cloud alternatives) that were part of the NSF Cloud decision. Furthermore, research also analyzed public documents presented by NSF to OMB related to Cloud initiatives at NSF.

Together, these investigational sources met the triangulation requisites of Chapter Three and supported the findings of this research project.

APPENDIX C: CASE STUDY 3 (VA) BACKGROUND

Introduction

This appendix provides additional background on the case study research into the May 2012 decision by Veterans Affairs (VA) to migrate their legacy email systems to cloud. The primary decision maker was Charles De Sanno, VA Executive Director of Enterprise Systems Engineering who led the decision-making process. The chief architect for the decision process was Franco Susi, Senior Systems Engineer for the VA Office of Information and Technology. A stakeholder and observer of VA's IT decisions was Ms. Lorraine Landfried serves as Veteran Affairs' Deputy Chief Information Officer (DCIO) for Product Development (PD).

The investigations for this case followed the methodology described in Chapter 3. VA's champion for this research investigation was Roger Baker, VA CIO. Baker also served as the executive decision maker for Cloud migration and other significant IT initiatives. The investigative sources for the case included De Sanno, Susi, and Landfried.

Some VA documentation – particularly public statements and acquisition documents about the Cloud migration also informed this case study investigation.

The Federal Organization – VA

The Department of Veterans Affairs (VA) was established as an independent agency under the President by Executive Order 5398 on July 21, 1930 and was subsequently elevated to Cabinet level on March 15, 1989. (VA 2014). The VA has a budget of $150B

and a workforce of 280,000. For this research project, VA fit the "large Agency" category.

VA considers themselves a customer service organization – to serve Veterans. Their customers are individuals who have served in one of the seven uniformed services and who meet the requirements prescribed by law for VA benefits. The largest service the VA provides is health care. They are the largest integrated health care delivery system in the US. (VA 2014) The second major service the VA provides is burials and memorials. The third service is actually a portfolio of additional services such as: education (e.g. GI Bill), loans, life insurance, and vocational rehabilitation. The VA is organized by those three services, however the VA CIO exercises centralized influence over IT investments through reviews, policy, budget authority, and approval authority.

Although headquarted in Washington DC, the VA has facilities across the US so that VA personnel are posted close to the Veterans they serve. (See Figure 61) VA's IT systems, including email, serve this large, federated, and distributed enterprise.

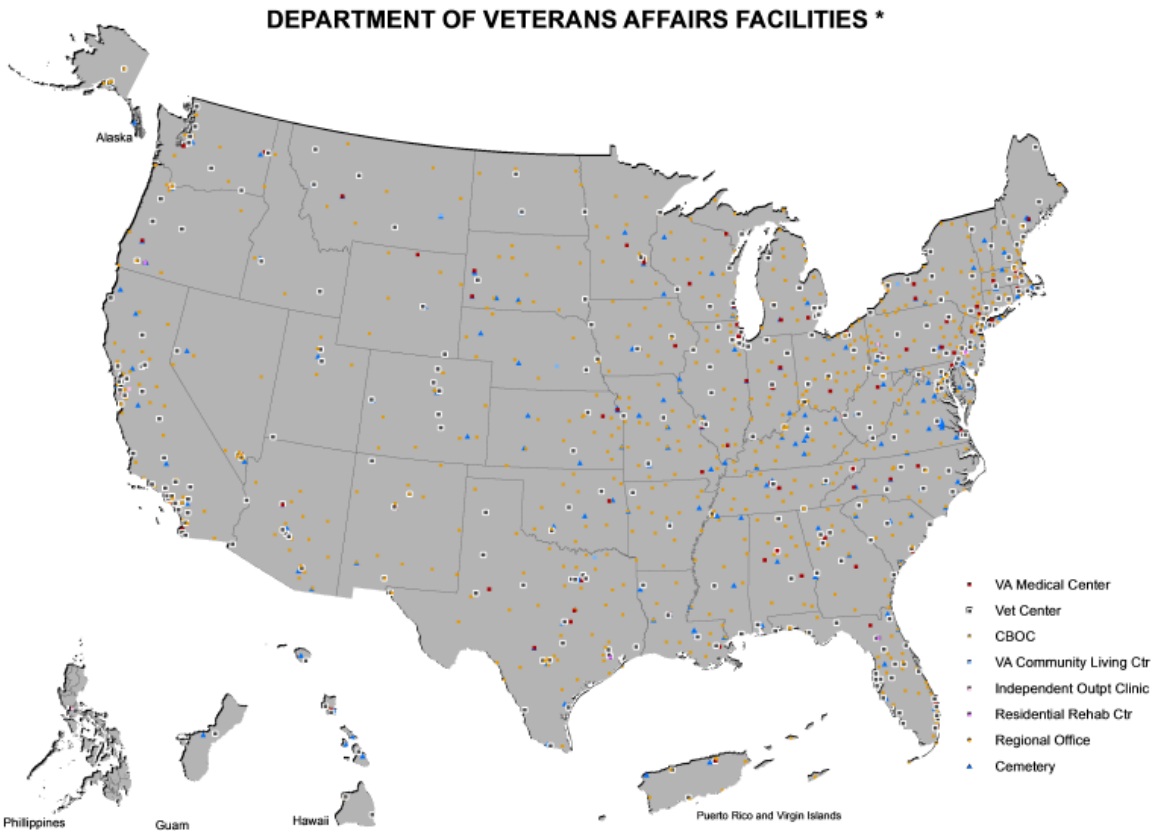


Figure 61 - VA facilities are scattered across the United States (VA 2014)

The Legacy IT System

VA's legacy email system was Exchange 2003 (except for one region that had upgraded to Exchange 2007). (Susi 2012) The VA hosted 32 instantiations of Microsoft Exchange running on about 300 servers across the enterprise. (Susi 2012) They had approximately 495,000 email accounts. This number was greater than the number of employees because Exchange requires accounts for resources such as conference rooms with public schedules hosted on Exchange. The legacy system stored 69 terabytes of data, yet even with that amount of data, users felt the email system restricted their productivity by limiting them to a small mailbox size.

The Cloud Decision

The Cloud migration decision itself was fairly informal. VA was outgrowing its email system. The VA was growing because the number of Veterans was growing and Congress enabled growth through increased funding. Yet the email system was seven years old, at the end of its lifecycle. VA had been able to ensure centralized configuration control over its 32 email clusters, but the distributed deployment was technically and managerially challenging. Implicitly, the decision leader knew that the status quo was a poor option. the two alternatives under consideration were VA-hosted email (centralized hosting, but with only some Cloud characteristics) and vendor-supplied email through a community Cloud. See Figure 62.

	Email Option	Description	- Owner - Operator	Cloud? - Deployment Model - Delivery Model
1	Current VA Email	Use existing (legacy Microsoft) Exchange 2003 (with possible technology refreshes)	- VA - VA using contractors	Cloud? No
2	VA-Hosted MS 365	Consolidate email into four datacenters running MS 365 email	- VA & MS - VA using contractors	Cloud? Slightly - Private SaaS
3	Cloud MS 365	Purchase email from a vendor hosting MS 365 to government customers	- Vendor - Vendor	Cloud? Yes - Community - SaaS

Figure 62 - VA Cloud Decision Alternatives

Decision Makers

The decision to migrate to Cloud was led by Charles De Sanno, VA Executive Director of Enterprise Systems Engineering, but the formal approval authority was the VA Chief Information Officer (CIO), Roger Baker. Baker also served as champion for this research project, orchestrating interviewees and authorizing access to releasable documents. Another stakeholder in the decision was Franco Susi, Senior Systems Engineering for VA Office of Information and Technology, who developed the analysis on the technical data and helped shape decision factors. John Hays, Director Systems Design and Core Services provided insight into the decision discussions. Lorraine Landfried, Deputy CIO for Product Development was a latecomer to the decision, but observed the final discussions and brought a fresh perspective from her previous assignment at the Department of Homeland Security.

Decision Process

The VA decision process was fairly informal, according to Charles De Sanno. (De Sanno 2015) Much of the effort focused on how to best procure the Cloud alternative. Subsequently that effort resulted in a Request for Information from industry followed shortly by a Request for Proposal and a contract award to a vendor.

Conduct of the Case Study (NSF)

This case study was conducted in accordance with the case study protocol described in Chapter 3. The researched included the following investigational sources:

- Charles De Sanno, VA Executive Director of Enterprise Systems Engineering,

- Franco Susi, Senior Systems Engineering for VA Office of Information and Technology, who developed the analysis on the technical data and helped shape decision factors.
- Lorraine Landfried, Deputy CIO for Product Development
- Researcher obtained and reviewed documents relating to the hosting alternatives (cloud alternatives) that were part of the VA Cloud decision. Furthermore, research also analyzed public documents presented by VA to OMB and Congress
- The researcher also benefited from background on the VA learned through advisory support to the VA's "Ruthless Reduction Task Force," a team chartered a year prior to identify ways to reduce the VA's IT expenditures.

Together, these investigational sources met the triangulation requisites of Chapter Three and supported the findings of this research project.

APPENDIX D: LETTERS AND FORMS

The next three pages of this appendix contains a sample of:

- Organization Sponsorship Request Letter
- Individual Interview Request Letter
- Study Collection Record

[EMAIL/LETTER TO CASE STUDY ORGANIZATIONS]

Subj: PhD Research (Historical Case Study) for <organization>…. Al Mink & <Name>

<Name>,
You may recall that I'm pursuing my PhD in Systems Engineering at GMU. I've completed academics, examinations, and assembled a renowned advisory committee (to include a former DoD CIO). Now I am embarking on an advanced research project that offers an organization an objective, transparent decision support model for selecting legacy IT systems to move to the Cloud.

I would interview your organization and research documents about a prior decision your organization made to migrate (or not migrate) to Cloud. The interviews and other research would use OMB's Cloud Strategy (publicly available) as a framework. I would perform this research as a PhD student (not as an SRA employee), leveraging Federal CIO guidance, DoD guidance, emerging academic thinking, and my personal expertise. This research and the interview questions would not expose me to sensitive information about future acquisitions – this is historical (past) research only.

Data collected from your organization for this research will be most powerful when it can be attributed directly to your organization in the final dissertation. However, this research project also contains provisions to provide confidentiality (non attribution) should you prefer.

Features of this approach:
- Complies with Federal & DoD guidance
- Incorporates Federal CIO's (OMB's) ***Value and Readiness*** cloud decision framework
- Leverages academic thinking and objectivity
- Exploits researcher with both strong knowledge of DoD's organizations and relevant technologies
- Focuses on actionable results

Benefits from this research:
Although no individual in your organization would accrue personal benefits from participating in this research, soft benefits to your organization and your leadership may include:
- After-the-fact reflection on a Cloud migration decision, providing better insights for future decisions
- Recognition in a published dissertation and related journal articles (assuming you permit attribution)
- Influence a body of knowledge that will likely affect Cloud decisions across all Federal Agencies
- Efficient use of resources because this is an academic project and the researcher is provided at no cost to you

<Short Name>, I hope I've intrigued you with this proposal. The impending federal timelines for cloud migration as well as my own PhD timetable indicate that this is the perfect time to explore this topic. The next step would be your endorsement for the research and your identification of a primary point of contact in your organization (preferably the individual who made the Cloud migration decision).

Very respectfully,

Al Mink

EMAIL/LETTER TO CASE STUDY INDIVIDUAL

Subj: PhD Research (Historical Case Study) for <Case Name>…. Al Mink & <Interviewee>

< Interviewee>,

<Organization Leader Name> indicated you were a key individual to provide research data about <Case Name> Thanks, in advance, for your support to this important research.

Background
I'm pursuing my PhD in Systems Engineering at GMU. I've completed academics, examinations, and assembled a renowned advisory committee (to include a former DoD CIO). Now I am embarking on an advanced research project that offers Federal Agencies an objective, transparent decision support model for analyzing legacy IT systems to move to the Cloud.

Your role in this important research:
Your support for this research would include interviews with you and others who contributed to the <case study name> as well as review of any documents relevant to the Cloud decision. These interviews and other research would be organized around OMB's Cloud Strategy (publicly available) as a framework. I will perform this research as a PhD student (not as an SRA employee), leveraging Federal CIO guidance, DoD guidance, emerging academic thinking, and my personal expertise.

Confidentiality:
Data collected from you for this research will be most powerful when it can be attributed directly to you and your organization in the final dissertation. However, this research project also contains provisions to provide confidentiality (non attribution) should you prefer.

Next Steps:
<Interviewee>, I hope you are enthused about your role in the project and the potential resulting from this research. The next steps would be to coordinate a time for this interview. The interview should be in-person and usually lasts 90 minutes. If you like, I can also arrange time to answer any pre-interview questions you might have – and we could do this preparation session by phone.

The impending federal timelines for cloud migration as well as my own PhD timetable indicate that this is the perfect time to explore this topic. Please let me know what date/time works best for us to meet.

Very respectfully,

Al Mink, PhD Candidate, George Mason University

CASE STUDY COLLECTION RECORD

Cloud Migration Al Mink

SOURCE INFORMATION

Agency/Organization	Case (Migration)	Role	Name/Title	Date Today	Date Originated	Remarks		

CONTEXT

What migrated	Effort ($)	Effort (users)	NIST Level (0-4)	Decision Date	Decision Maker	Decision	Status Today	

DECISION FACTORS

FACTOR	Relevant (No Prompt)	Relevant (Prompted)	Definition	Most Important?	Data Collected?	What Collected?	How depicted?	Validation Collection?
Efficiency								
Agility								
Innovation								
Value - Other								
Security								
Service Characteristics								
Market Characteristics								
Net App & Data Read.								
Government Readiness								
Technology Lifecycle								
Readiness - Other								

Decision Structure?								
DS Categories								

Decision Question?								
DQ Alternatives								

Anything missing?								
Anything unneeded?								

APPENDIX E: ARAUCARIA DATASET

A dataset for this research project accompanies this report. The dataset contains the nodes referencing the source data as well as the intermediary circumstantial nodes and inference links leading up to the ultimate probanda.

The dataset is in Araucaria Markup Language (AML), a conforming variant of eXtensible Markup Language (XML). (Reed 2004)

See http://araucaria.computing.dundee.ac.uk/doku.php for information about obtaining and using Araucaria.

REFERENCES

Alliance, C. S. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing. V2.1.

Army (2005). Field Manual 1. U. Army. Washington DC. FM 1: 2-26.

Army (2008). Analysis of Alternatives (Initial Draft for Enterprise Email), US Army.

Army (2012). Attestation Review of Enteprise E-mail Cost-Benefit Analysis. Defense, U.S. Army AUdit Agency.

Army (February 2012). Enterprise Email, Army Service Acquisition, Report to Congress. D. o. t. Army.

Army Force Management School, A. (2010). DoD Planning, Programming, Budgeting, and Execution (PPBE) Process -- Executive Primer. Army, Army Force Management School.

Army, U. (2010). "Army launches enterprise email: DISA will implement." The Official Homepage of the United States Army Retrieved Sep 24, 2011, 2011.

Army, U. (2012). "The Offical Homepage of the United States Army." Retrieved 8/26/2012, 2012.

AT&L, U. (2003). Defense Acquisition System. Defense, DoD.

Barclay, P. (2010). Email Routing Flow, US Army.

Barclay, P. (2012). Interview with LTC Peter Barclay.

Baskerville, R. L. (1999). "Investigating Information Systems with Action Research." Communications of the Association for Information Systems **2**(19).

Burrelli, D. F. (2012). FY2012 National Defense Authorization Act: Selected Military Personnel Policy Issues. 7-5700.

Bussey, J. (2011). "Seeking Safety in Clouds." Wall Street Journal(September 16, 2011): B8.

Carlock, P. a. F., R (2001). "Systems of Systems (SoD) Enterprise Systems Engineering for Informatio-intensive Organizations." Systems Engineering **4**(4): 242-261.

Chandler, A. a. C. J., Ed. (2006). A Nation Transformed by Information: How Information Has Shapted the United States from Colonial Times to the Present, OUP USA.

Committee on Veterans' Affairs, U. S. (2013). Hearing before the Committee on Veterans' Affairs before the United States Senate. Committee on Veterans' Affairs. Washington, DC.

Congress (2006). National Defense Authorization Act for Fiscal Year 1996. Congress. Washington, DC, Government Printing Office.

Congress, U. (1950). National Science Foundation Act of 1950. Public Law 507. U. Congress. Washington, DC, Government Printing Office. **S247**.

Congress, U. (2011). National Defense Authorization Act for Fiscal Year 2012. Government Printing Office, Government Printing Office. **Public Law 112-81**.

Council, F. C. (2010). Proposed Security Assessment & Authorization for U.S. Governent Cloud Computing. F. Government. Washington, DC. **Draft Version 0.96**.

Courts, U. (2011). Google and Onix Networking v The United States and SoftChoice Corporation. 10 - 743C. T. U. S. C. o. F. Claims. Washington, DC, US Government Printing Office. **10 - 743C**.

Coxe, R. (2000). Evaluation of Army Knowledge Online. A. Mink. Ft Belvoir, VA.

Creswell, J. W. (2005). Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research. Upper Saddle River, NJ, Prentice Hall.

CSIS (2009). Forum on Cloud Computing. Center for Strategic and International Studies Forum on Cloud Computing.

Davis, F. D. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." MIT Quarterly **13**(3): 319.

De Sanno, C. (2012). Interview with Charles De Sanno. A. Mink. Washington, DC.

De Sanno, C. (2015). Follow-up Interview with Charles De Sanno. A. Mink. Washington, DC.

DISA (2011). DCO Users and Meeting Minutes for March 2011. Defense, Adobe Groups.

DISA. (2011). "Rapid Access Computing Environment (RACE)." Retrieved September 25, 2011, 2011, from http://www.disa.mil/computing/cloud/race.html.

DISA, D. I. S. A.-. (2007). "Solicitation HC1047-07-R-0027 NCES." FedBizOps Business Opportunities Retrieved June 24, 2007, 2007, from https://www.fbo.gov/index?s=opportunity&mode=form&id=86a855b47020ce8f2a33e0aeb839e10f&tab=core&_cview=0.

DISA, D. I. S. A.-. (2011). "Cloud Computing & Enterprise Services." DISA Web.

DISA, P. D. (2011). Defense Connect Online (DCO) Award Notice. FBO. DoD, Federal Biz Ops (FBO).

DoJ, D. o. J. (2001). "IX. Agencies Listed by Size Categories." Section 508 of the Rehabilitation Act (Results of 2001 Survey) Retrieved 3/27/2015, 2015, from http://www.justice.gov/crt/508/report2/agencies.php.

FCW (2012) "Federal 100: Lt Col Peter C. Barclay." Federal Computer Week: STrategy and business management for government leaders.

Forrest, W. (2009). "Clearing the Air on Cloud Computing." McKinsey **April 2009**.

Friedman, G. and A. P. Sage (2003). "Case Studies of Systems Engineering and Management in Systems Acquisition." Systems Engineering **7**: 84-97.

GAO, G. S. A. (2005). Federal Acquisition Regulation. 48. GSA. Washington, DC, Government Printing Office.

Gartner (2008). "Gartner Says Contrasting Views on Cloud Computing are Creating Confusion." Garnter Newsroom.

Gartner (2011). "Cloud Computing." IT Glossary.

Gentry, C. (2011). "Homomorphic Encryption, Making Cloud Computing More Secure." Technology Review(May/June 2011).

Government Accountability Office, G. (2012). Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned. Washington, DC, Self.

Government, U. (2002). E-Government Act of 2002. Legislative. Washington, DC, Government Printing Office. **Public Law 107-347**.

GSA (2011). Cloud Computing Brochure. U. G. S. Administration. Washington, DC, GSA.

GSA, G. S. A. (2010). GSA Becomes First Federal Agency to Move Email to the Cloud Agencywide. Washington, DC, GSA.

Hale, J. (2011). DoD Enterprise Email. DISA Customer & Industry Forum. Baltimore, MD.

Horton, J. (2012). Interview with Jerry Horton, CIO of USAID. A. Mink. Washington, DC.

IMJ (2010). "Federal Govt. Still Wary of the Cloud." Information Management Journal **44**(4): 15.

Ipiotis, N. (2010). Email Options. Powerpoint. E. Options. Arlington, VA, NSF.

Ipiotis, N. (2012). Interview with Nick Ipiotis (NSF). Researcher.

Ipiotis, N. (2013). "Linked-In." Retrieved April 29, 2013, 2013, from http://www.linkedin.com/in/nikolaosipiotis.

Kadane, J. a. S., D (1996). A Probabilistic Analysis of the Sacco and Vanzetti Evidence, John Wiley & Sons, Inc.

Kider, L. J. C. (1986). Research methods in social relations. New York, Holt, Rinehart & Winston.

Killaly, M. (2011). I Can, but I won't: An Exploratory Study of People and New Information Technologies in the Military. Masters Submission (not yet approved), Air Force Institute of Technlogy.

Kundra, V. (2010). 25 Point Implementation Plan to Reform Federal Information Technology Management. C. I. Officer. Washington, DC, The White House. **December 9, 2010**.

Kundra, V. (2010-2). Cloud Computing: Benefits and Risks of Moving Federal IT into the CLoud. Legislative. Washington, Government Printing Office. **111th Congress, Secod Session**.

Kundra, V. (2010-2). Federal Data Center Consolidation Initiative (FDCCI). OMG. Washington, DC, Federal CIO. **February 26, 2010**.

Kundra, V. (2011). Federal Cloud Computing Strategy. U. S. C. I. Officer. Washington, DC, White House**:** 1-39.

Landfried, L. (2012). Interview with Lorraine Landfield, Veteran Affairs' Deputy Chief Information Officer (DCIO) for Product Development (PD). A. Mink. Washington, DC.

Leader, N. S. (2012). Interview with (unamed) NSF Senior Leader. A. Mink. Arlington, VA.

Louridas, P. (2010). "Up in the Air: Moving Your Applications to the Cloud." IEEE Software **27**(4): 6.

Martin, J. (2006). An Enterprise Architecture Process Incorporating Knowedge Modeling Methods. PhD Doctorial, George Mason University.

Mazmanian, A. (2014). "How VA's $36 million move to the cloud evaporated." Federal Computer Week.

McAfee, A. a. B., Erik (2011). "What Makes a Company Good at IT?" Wall Street Journel: R3.

McClure, D. (2012). Interview with Dave McClure, Associate Administrator for Citizen Services & Innovative Technologies. A. Mink. Washington, DC.

McLure, D. (2011). The Next IT Revolution? Cloud Computing Opportunities and Challenges. S. House Science, and Technology Committee, Subcommittee on Technology and Innovation. Washington, DC.

Mink, A. (2011-2). Interview with FAA on Cloud. Washington, DC.

Mink, A. L. (2010). Planning Records. Defending a Private, Enterprise Cloud in a Hostile Environment, Johns Hopkins Kossiakoff Center, Maryland, Armed Forces Communications and Electornics Association (AFCEA).

Mink, A. L. (2011). What's Real about Cloud for USAF: The Truth About Cloud from Analyzing Cloud Implementations. Air Force Information Technology Conference. P. BES. Montgomery, AL.

Morton, T. A. a. G. (2009). The Economics of Cloud Computing: Addressing the Benefits of Infrastructure in the Cloud. McClean, Virginia, Booz, Allen, & Hamilton.

Motsing, K. (2012). GMU HSRB Not Research Protocol #7946. G. Office of Research Subject Protections. GMU. **7946**.

NIST, N. I. o. S. T.-. (2011). The NIST Definition of Cloud Computing (Draft). P. a. G. Mell, Timothy, National Institute of Standards and Technology.

Northcutt, A. (2012). Interview with Amy Northcutt (NSF). A. Mink. Arlington, VA.

NSF (2010). Email Options. PowerPoint. E. Options. Arlington, VA.

NSF (2010-2). NSF Exhibit 300: Capital Asset Plan and Business Case Summary. Arlington, VA, US IT Dashboard.

NSF (2011). Empowering the Nation Through Discovery and Innovation: NSF Strategic Plan for Fiscal Years (FY) 2011-2016. I. F. Agency. Arlington, VA, Self.

NSF. (2013-1). "About the National Science Foundation." 2013, from http://www.nsf.gov/about/.

NSF. (2013-3). "NSF Office of Information and Resource Management." Retrieved APr 29, 2013, 2013, from http://www.nsf.gov/oirm/cio.jsp.

NSF (Dec 2010). "Quick Win" Pilot Options, NSF.

Olson, A. (2009). Enterprise Messaging and Collaboration Services Request for Information. U. A. P. EIS. Ft Belvoir, Federal Business Opportunities

OMB (2009). Fiscal Year 2009 Report to Congress on the Implemenation of the Federal Information Security Management Act of 2002. O. o. M. a. Budget. Washington, DC**:** 28.

OMB (2011). Agencies Have Identified 78 Systems Migrating to the Cloud Within One Year.

OpenCrowd. (2010, 6/8/2010). "Cloud Taxonomy." Retrieved 9/20/11.

Oprea, A. (2011). "Guaranteeing Cloud Security." Technology Review **114**(5): 45.

Orlikowski, W. J. (1991). "Studying Information Technology in Organizations: Research Approaches and Assumptions." Information System Research **2**(1): 1-28.

Orndorff, M. (2010). Technical Exchange: Defending the Cloud in a Hostile Environment. Armed Forces Communications and Elctronics Association (AFCEA), Johns Hopkins Applied Physics Laboratory, Maryland, AFCEA.

Pavlou, P. (2003). "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk wiht theTechnology Acceptance Model." Internaional Journal of Electronic Commerce **7**(3): 69-103.

Peak, D. A., Guynes, Carl S.; Prybutok, Victor R.; Xu, Chenyan (2011). "Aligning Information Technology with Business Strategy: An Action Research Approach." Jounel of Information Technoloyg Case and Application Research **13**(1): 16.

Pizette, G. R. a. L. (2010). "Federal Cloud Computing - A Decision Process for Applying Cloud Computing in Federal Environments." MITRE **March 2010**(Revised August 2010).

Plant, R. (2011). "To Cloud, or Not to Cloud." Wall Street Journal(April 25, 2011): R9.

Reed, C. a. R., G (2004). Araucaria: Software for Argument Analysis, Diagramming, and Representation, Division of Applied Computing, University of Dundee.

Schramm, W. (1971). Notes on case studies of instructional media projects. Working paper for the Academy for Educational Development. Washington DC, Academy for Educational Development.

Schum, D. (2009). Research Methods in SEOR and Information Technology. Fairfax, Virginia, Course Material.

Sibley, E. H. (1985). "How to Select and Evaluate a DBMS." The Journal of Information Systems Management **2**(2): 40-49.

Simpson, D. G. (2011). DISA Leeter Estimate (LE) VA Veterans Information System and Technology (VistA) Defense Enterprise Computing Center (DECC) Migration. DoD. Ft. Meade, MD, Defense Infromation Systems Agency. **September 2, 2011**.

Sorenson, J. (2012). Interview with LTG Jeffrey Sorenson. A. Mink. Reston, VA.

Stake, R. E., Ed. (2006). Multiple Case Study Analysis, Gilford Press.

Strassmann, P. (2011). "Shifting to Infrastructure-as-a-Service?" Strassmann's Blog 2011.

Susi, F. (2012). Interview with Franco Susi. A. Mink. Washington, DC.

Takai, T. M. (2013). Designation of the Department of Defense Enterprise Email as an Enterprise Service for the Joint Information Environment. D. CIO. Washington, DC, DoD CIO. **Memo dated Sep 5, 2013**.

Tara Behrend, E. W., Jennifer London, Emily Johnson (2011). "Cloud computing adoption and usage in community colleges." Behaviour & Information Technology **30**(2): 231.

TechAmerica (2011). Leveraging Technology: To Improve the Performance of the Government. Twenty-First Annual Survey of Federal Chief Information Officers.

USAID (2011). Google Mail Deployment. USAID. Washington, DC, USAID. **1**.

USD(AT&L) (2008). Operation of the Defense Acquisition System. 5000.02. A. L. Department of Defense. Pentagon, DoD. **5000.02**.

USG. (2012, October 2012). "A-Z Index of U.S. Government Departments and Agencies." Government Made Easy.

USG, U. G. (2015). "A - Z Index of U.S. Government Departments and Agencies." The U.S. Government's Official Web Portal. Retrieved 4/26/2015, 2015.

USPTO (1999). Trademark Document Retrieval for Serial Number 75291765. Commerce, US Patent and Trademark Office.

VA, V. A.-. (2011). Hosted Cloud Enterprise Exchange, Archive, Backup, and Storage System (RFI). Washington, DC.

VA, V. A.-. (2014). FY 2014-2020 Strategic Plan. V. Affairs. Washington, DC, VA.

Vafopoulos, M. N., Gravvanis, G. A. and Platis, A. N., (2007). "New Directions in Computing on Demand (CoD) " Hellenic European Research on Computer Mathematics & Conference its Applications **September 2007**: 1.

Vietmeyer, R. (2011). "Forge.mil: A DoD Innovation for the Enterprise." Retrieved September, 24, 2011, 2011.

West, D. M. (2010). Saving Money Through Cloud Computing. Governance Studies, Brookings Institute. **Special Report**.

Wigmore, J. (1937). The Science of Proof: As Given by Logic, Psychology, and General Experience and Illustrated in Judicial Trials. Boston, MA, Little, Brown.

Winans, T. B. a. B., John S (2009). "Moving Information Technology Platforms to the Clouds: Insights Into IT Platform Architecture Transformation." Journal of Service Science **2(**2): 32.

Wynne, M. (2010). "IT-AAC ROADMAP FOR SUSTAINABLE ACQUISITION REFORM." IT Acquisition Advisory Council.

Yin, R. K. (2003-2). Case Study Research: Design and Methods. Thousand Oaks, CA, Sage Publications.

Yin, R. K. (2009). Case Study Research: Design and Methods. Thousand Oaks, SAGE Inc.

Yin, R. K. (2012). Applications of Case Study Research. Thousand Oaks, CA, Sage Publications.

CURRICULUM VITAE

Allan L. Mink II is a senior leader and published author focused on strategic issues in DoD technologies. He possesses over 25 years' experience in information technology, strategic planning, program/project management, fiscal management, and operations in government and industry. His government responsibilities spanned OSD, Joint, and all USAF. He reported to most senior DoD leadership in duties as Executive Officer to the Vice Chief of Staff and as Senior Military Assistant to the Undersecretary of Defense. Mr. Mink led source selection advisors for multi-year $100M contracts. As Chief of USAF IT Initiatives for the AF CIO, he implemented enterprise IT initiatives throughout the USAF, increasing worldwide operational effectiveness, improving morale, and reducing the costs of day-to-day business for a 750,000-person, $100B enterprise. Mr. Mink is a Gulf War Veteran and combat-tested pilot with 3,000 flight hours.

Mr. Mink currently is the Managing Partner of Systems Spirit, a boutique consulting firm connecting technology innovators with the needs of Federal IT leaders. During his previous positions at SRA International and Unisys Corporation, Mr. Mink built a new business unit at CEO's direction creating a $150M+ revenue stream from scratch in nine months while serving as Vice President, Defense & Intelligence. He led a 500+ person, $60M+ annual practice that developed solutions ranging from financial consulting and architecture to managed services and IT infrastructure. He was awarded the coveted Unisys Gold Medal for business growth.

Mr. Mink is active in industry associations, including Past President of Northern VA Chapter of AFCEA, Chairman of AFCEA International Solutions Committee, and is member of the Systems Engineering Committee of NDIA. He served as Past President and Chairman of region's Enterprise Forum, and advisor to the Entrepreneur Center of NVTC. He's as a contributing member of Virginia CTO Round Table.

Mr. Mink has an undergraduate degree in Computer Science from MIT, an MBA from Carnegie-Mellon, two recent Fellowships from MIT & Stanford, and is pursuing PhD in Cloud-related research at George Mason University. He chaired DISA's technology exchange on Cloud Security and has hosted DoD topics for the Cloud Security Alliance. He's provided seminars on Cloud-related topics to the technical members of the Joint Staff and Veterans Affairs.