Planning & Management Methods for Migration to a Cloud Environment

Author: Donn K. Kearns

December 2017

Department No.: T863
McLean, VA

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release; Distribution Unlimited. Case Number 17-4029

MITRE

This page intentionally left blank.

Executive Summary

The purpose of this document is to introduce and describe a set of high-level planning and management concepts and approaches to support efforts to migrate a data center (e.g., services, applications and data) to a cloud-based architecture. It identifies and introduces a variety of "best practice" management approaches to help a project manager begin the planning process and to manage key aspects of its execution and operation. While it is focused on cloud migration activities, much of the content is applicable to planning any large-scale, complex Information Technology (IT) transformation.

The primary target audience is an organization or a team who intends to migrate its data services from a local data center to a cloud environment but may not be experienced in planning such a large-scale migration. It is not aimed at qualified acquisition program managers who are trained, certified, and experienced in such activities. Further, it is not a technical document, and does not address the technical aspects of migration activities.

This document was written and is maintained by the Computing Infrastructure and IT Service Management Department (T863) within the MITRE Infrastructure and Engineering Technical Center (T860). Within this Center, the Computing Infrastructure and IT Service Management Department (T863) is available for consultation on any initiatives that may utilize or depend on its core capabilities.

This page intentionally left blank.

Table of Contents

List of Tables

List of Figures

Planning and Management Methods for Migration to a Cloud Environment

1. Purpose and Scope

Migrating to a cloud environment, or any other large-scale IT transformation, is a highly complex undertaking. It requires significant upfront thought and in-depth planning to ensure effective resource use and risk management, on-time and within budget implementation, and ultimately operational success. Without a standardized approach to planning (e.g., a planning template), each organization must independently create its plan from scratch. Such an approach is inherently inefficient, slow, and duplicative of similar work done elsewhere. In addition, it may not fully leverage lessons learned and/or best practices from other activities, and may be risky due to possible oversights. This problem is compounded if personnel in charge of the migration are not experienced in planning complex IT projects.

This document describes ways to develop an effective and efficient planning approach, and helps provide a roadmap for an inexperienced team. Its purpose is to introduce and describe a set of high-level planning and management concepts and approaches to support efforts to migrate a data center (e.g., services, applications and data) to a cloud-based architecture. It identifies and introduces a variety of "best practice" management approaches to help a project manager begin the planning process and to manage key aspects of its execution and operation. While it is focused on cloud migration activities, much of the content is applicable to planning any large-scale, complex Information Technology (IT) transformation.

It identifies a broad list of considerations to help federal organizations "jump-start" their planning process. It is generic in nature because it is not focused on a specific customer or solution, but rather on high level concepts and factors to help ensure important migration issues are not overlooked. In reviewing them, if a given concept/factor is not applicable after consideration, it can be discarded. If it is applicable, however, the implementing organization needs to assess its impact, define a plan to address it, and then manage the plan.

This is not a technical document. Rather, it focuses on the planning and management aspects of a migration and not the technical aspects. The primary target audience is an organization or a team who may not be experienced in planning cloud migration or other large-scale IT projects. It is not intended for qualified acquisition program managers who are trained, certified, and experienced in such activities.

It assumes (and therefore does not address) that organizational leadership has made the decision for such a consolidation/ migration. It further assumes the reader is familiar with the basics of data center operations and cloud computing.

2. Introduction to Cloud Computing

Operating in a very dynamic and cost-constrained environment, the Federal Government must respond continually to operational challenges such as changing/evolving requirements; optimizing, operating, sustaining, and replacing outdated and costly IT; and addressing ever-increasing security and privacy threats. Often, federal organizations must leverage new IT capabilities to address these challenges. Although technologies can provide effective, efficient, and timely solutions, the availability of the necessary resources (e.g., funding) to address them is typically limited and increasingly constrained. Given this environment, the Federal Government is seeking to provide best practices and guidance on using IT to better achieve operational objectives while reducing risks and costs.

Federal guidance, such as the Office of Management and Budget's (OMB) Data Center Optimization Initiative (DCOI)[1], seeks to transition IT operations to a more efficient infrastructure by leveraging technology advancements such as cloud services. Federal organizations have been directed to reduce the numbers of data centers through consolidation.[2] Consolidation (to include leveraging cloud services) can offer the following benefits:

- Provide high availability, scalability, and elasticity to support "service on demand" in terms of providing services that are available when and where needed, and that can quickly expand or reduce the use of resources (to include costs) as requirements dictate.

- Provide agility in operational response by leveraging existing capacity as well as available technologies such as Software Defined Networks (SDNs) to reduce the time needed to stand up mission-specific, time sensitive, ad hoc architectures.

- Reduce the acquisition, Operations and Maintenance (O&M), and sustainment costs of data center operations through resource pooling and economies of scale. These costs include those associated with hardware, software, personnel, facilities, etc. Resource savings can then be used to support other priority functions.

- Increase security through more centralized control of access to internal infrastructure as well as external networks.

- Allow supported organizations to focus on their mission instead of the acquisition, operations, and maintenance of IT services/infrastructure.

- Provide a measured service in which cloud customers only pay for the services they use.

- Enhance Continuity of Operations (COOP) or Disaster Recovery (DR) plans.

[1] OMB Memorandum M-16-19.

[2] CIO.Gov, "Data Center Consolidation and Optimization" (https://cio.gov/drivingvalue/data-center-consolidation/).

As data centers are consolidated, organizational leadership must decide what IT services should be provided, and from where; e.g., an in-house, locally owned and operated data center; an internal or external organization (federal or commercial vendor) that provides such services (i.e., the "cloud"); or a hybrid model. Cloud services may include the following, as defined in the National Institute of Standards and Technology (NIST) Cloud Computing Reference Architecture:[3]

- **Software as a Service (SaaS).** "The capability provided to the consumer is to use the providers applications running on a cloud infrastructure. The applications are accessible from various client devices 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."

- **Platform as a Service (PaaS).** "The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages 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 over application hosting environment configurations."

- **Infrastructure as a Service (IaaS)**. "The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)."

Figure 1 below from the NIST Cloud Computing Reference Architecture provides examples of SaaS, PaaS, and IaaS cloud services.

[3] *NIST Cloud Computing Reference Architecture*, National Institute of Standards and Technology (NIST) Special Publication 500-292, September 2011.

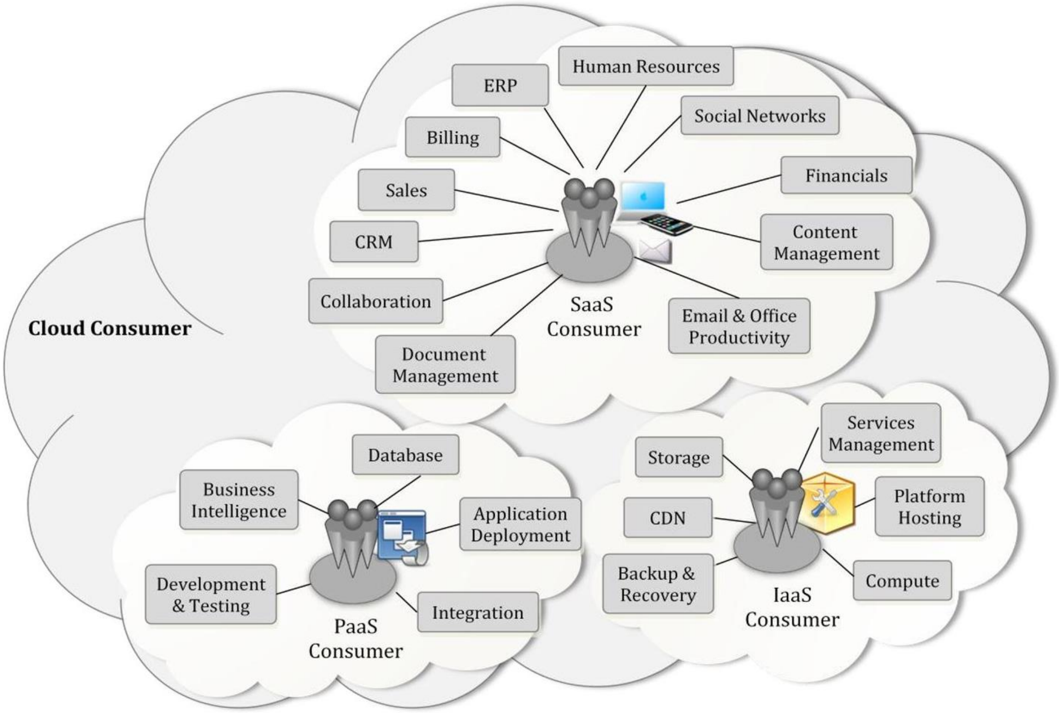


Figure 1. Cloud Services

Access to cloud computing technologies has greatly increased in the last few years with major vendors such as Amazon, Google, Cisco, and IBM providing cloud offerings. Government organizations, such as the Navy and the Air Force, have awarded large contracts for cloud services, and other federal organizations are planning such migrations to include the Social Security Administration, Veterans Administration, and the US Intelligence Community.

In determining what cloud service(s) to undertake, organizational leadership must consider costs, schedule, and performance factors to ensure the services:

- Meet business needs with services that are equal to or better than those previously provided (e.g., reliable, highly available, resilient, and secure).

- Increase efficiencies, which leads to reduced acquisition, operating, and sustainment costs (hardware, software, personnel, etc.), allowing savings to be re-allocated to other priorities.

In addition to these “hard” factors that are definable and measurable, leadership must take into consideration “soft” factors that bear on the success of the migration project. Because of the broad, transformational nature of such projects, they can have a significant impact on the organization and its personnel. For example, they can change roles, responsibilities, and workplace culture; cause staff disruption and uncertainty; impact IT service delivery processes; and require adaption to new technology. While these soft factors are not easily defined and measured, they can have a major adverse impact if not properly managed.

The likelihood of a successful consolidation or cloud migration can be greatly increased with detailed and focused upfront planning to develop a comprehensive migration plan, as well as continuous and pertinent communications among all stakeholders. This document identifies key planning and communications factors to help “kick start” and effectively scope the planning process. The information and approaches presented are focused on data center migration to cloud services, but they are generally applicable to planning any large-scale IT project.

3. Planning Approaches

This section describes several disparate approaches to help define, optimize, and manage a migration plan. It first discusses frameworks, which provide an overarching context for the project in terms of how to define and manage it. Next, given a defined project or solution, it describes an approach to identify gaps or redundancies that may cause implementation or operational problems, increase costs, delay implementation, or generally result in a sub-optimal or non-responsive solution. Throughout the project, but particularly in the early planning phases, major decisions need to be made based on an objective, data-driven approach. The next section provides such an approach using an analysis of alternatives to make critical decisions. The final section discusses how to establish specific tasks, timelines, and accountabilities to manage the project.

3.1 Frameworks

Federal organizations that intend to consolidate data centers and/or migrate into a cloud environment have common planning considerations/factors that need to be addressed. Tailoring a standard planning process and framework for this migration will reduce planning time and required resources, help ensure the appropriate planning factors are considered, and in general increase the likelihood of success.

The primary intent of using a framework is to ensure a thorough, well-thought-out, and manageable approach for planning and executing a migration project, as well as sustaining the capability once it goes operational. A framework can help in identifying and interlinking planning components to help ensure efficiency, effectiveness, and consistency within these areas, as well as identify interrelationships between the planning areas. For example, changes in data requirements may drive the need for new IT processes and technology, which can impact organizational responsibilities, all of which may drive the need for new policies or instructions (governance).

Four “best practice” frameworks are described below, with descriptions and/or references identified for more in-depth review. These frameworks may be applied across the entire planning, implementation, or operations phases, or they may best be used within specific phases (as described in Sections 4.1.1-4.1.5 below).

The four frameworks described below are the:

- Work Breakdown Structure (WBS) framework.
- IT Infrastructure Library (ITIL).

- Department of Defense Enterprise Service Management Framework (DESMF).
- Portfolio, Program, and Project Management Maturity Model (P3M3).

These frameworks can be overlapping in that elements of one framework can be used to build out another. For example, the categories of the ITIL, DESMF, or P3M3 frameworks can be used to populate the WBS. The processes that comprise those ITIL categories could represent the next level of decomposition with individual processes in each representing a further decomposition.

Arguably, of these frameworks, the WBS provides the most flexibility in defining the scope and activities associated with a given migration effort. Much of the underpinning of this document is based on a WBS approach.

3.1.1 WBS Framework[4]

The WBS provides a logical approach and framework to identify and manage all necessary activities across the planning, development, and implementation phases of a project. It takes a high-level set of categories and continually decomposes them until they reach a level of detail that allows for identification and management of specific activities. It can also be used as a framework for costing and establishing a master schedule (as described Section 4.4).

A WBS approach provides several significant benefits:

- **Management by objectives.** It forces detailed planning for determining the “who, what, when, where, why, and how” of the migration as well as developing a road map.

- **Activity management.** It establishes a way to identify and track specific activities so that they are identified and managed, and nothing is overlooked.

- **Definition of Responsibilities.** It provides a way to specify the roles for each activity thereby avoiding questions of responsibility and accountability.

- **Allocation of workload.** It helps ensure workload is fairly distributed across the migration team.

- **Consistency.** It enables consistency and thoroughness in planning and implementation by leveraging lessons learned from other implementations and best practices from the Federal Government and industry.

[4] Using a WBS is a standard project management technique, and is documented in many references such as the Project Management Institute’s Project *Management Book of Knowledge*, the International Council on Systems Engineering (INCOSE) “Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities,” and The MITRE Corporation’s *System Engineering Guide* (Attachment 4 provides linkages to these materials).

- **History.** It captures the history of the migration and provides “lessons learned” and “best practices” for similar efforts.

To demonstrate the development of a WBS, the high-level framework categories (Tier 1 of the WBS) shown below are: Planning, Processes, Technology, Data, Governance, Organizational Impacts, and Facilities (note that there are numerous logical ways to define the top tiers of a WBS, and this is just one example). Each of these areas is further decomposed into sub-categories that provide a view of activities at a lower level of detail. Sub-categorization continues to a level at which no more collective categories are needed, and instead, specific actions can be identified. These actions can then be associated with task leads and projected completion dates yielding an implementation (transition) plan, checklists, and schedule for management and tracking purposes. Figure 2 below depicts a notional WBS based on the above-described breakdown.

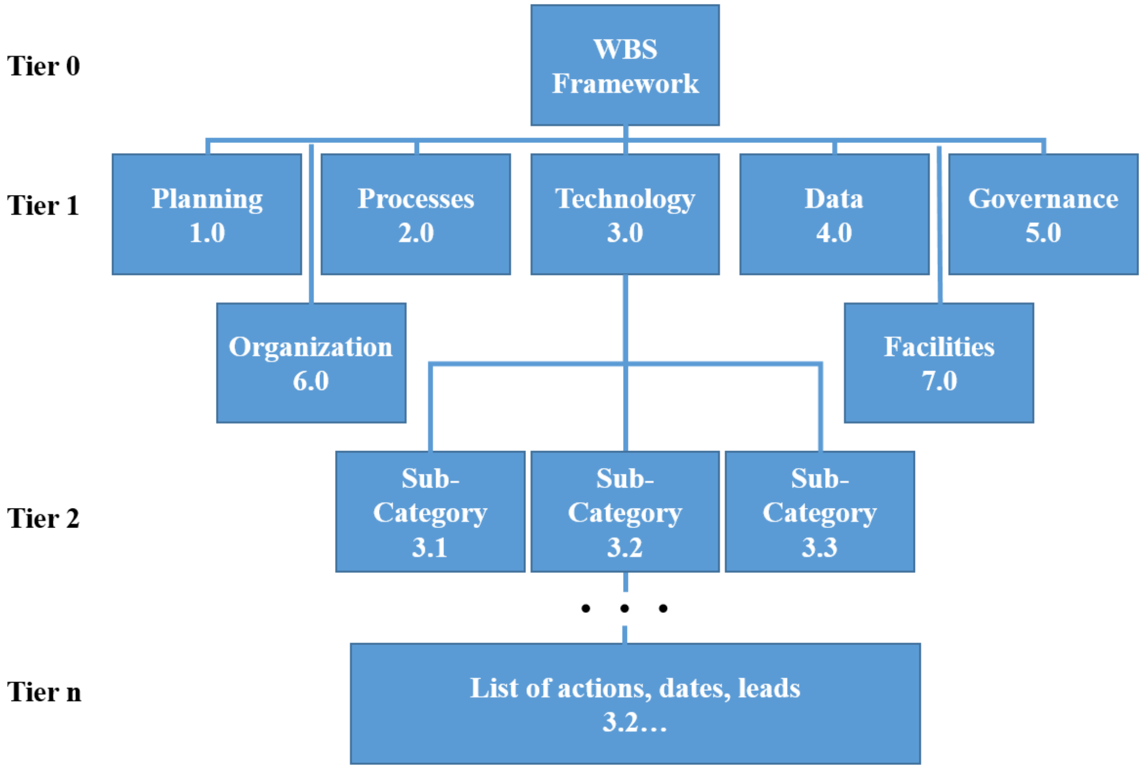


Figure 2. WBS Framework

3.1.2 ITIL Framework[5]

ITIL provides guidance on, and a framework for, implementing “best” business practices for IT Service Management (ITSM) and service delivery. It provides a good baseline of processes to

[5] *An Introductory Overview of ITIL® 2011*, The IT Service Management Forum (https://www.tsoshop.co.uk/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf).

develop and manage IT service delivery across the planning, developmental, implementation, and operational phases of a project, and is widely used within the US Government and industry as well as internationally. ITIL processes are the basis for Section 6, Processes.

The ITIL framework consists of five broad phases as listed in Table 1 below, each representing a stage of the ITIL service lifecycle. Each category includes a set of related processes, which are discussed in Section 6 and listed in Table 5. Details on ITIL are included at the hyperlink in footnote 6.

Table 1. ITIL Framework

ITIL Phase	Phase Intent
Service Strategy	• Develop/define a plan to satisfy a mission or business problem. • Identify needed assets.
Service Design	• Ensure that new or modified services satisfy the changing requirements of the mission or business. • Convert requirements from Service Strategy into designs to meet mission/business objectives.
Service Transition	• Ensure the new/modified services meet mission/business objectives. • Ensure services conform to Service Strategy and Design objectives.
Service Operation	• Provides services that meet Service Level Agreements (SLAs). • Manage IT that enables service delivery.
Continual Service Improvement	• Ensure quality and increase maturity of service provisioning through continual evaluation and improvement

3.1.3 DESMF[6]

The Department of Defense (DoD) Chief Information Officer (CIO) established the DESMF as the authoritative, integrated framework for addressing DoD services and processes. The intent of this framework is to enhance the ability of DoD organizations to implement, monitor, and improve IT service management and delivery. It leverages best practices from multiple frameworks, but is heavily ITIL-influenced. DoD organizations should consider this framework for their service delivery model. Like the ITIL framework, it can help develop and manage IT service delivery across the planning, developmental, implementation, and operational phases of a project.

3.1.4 P3M3 Framework[7]

This framework looks at process maturity across and within Portfolios, Programs, and Projects (P3), the competencies of the personnel who apply the processes, the supporting tools, and the

[6] *Department of Defense (DoD) Enterprise Service Management Framework (DESMF), Edition III,* DoD Chief Information Officer, 4 Mar 2016 (http://dodcio.defense.gov/Portals/0/Documents/DESMF%20EDITION%20III%20Signed%20June2016.pdf).
[7] *Introduction to P3M3, Version 3,* Axelos, July 2016 (https://publications.axelos.com/p3m3/Guide/Introduction.aspx).

information necessary to manage the processes. The P3 Management Maturity Model (P3M3) can be used to assess the maturity of an organization's management processes. It provides another angle from which to view the planning and management of the migration activity as well as assessing the follow-on operations.

In the context of P3M3, portfolios are comprised of related programs, and programs are comprised of related projects. P3M3 provides a good framework for organizations use a P3 approach to help manage their service delivery.

P3M3 looks at seven process areas common to Portfolio Management, Program Management, and Project Management. They listed in Table 2.

Table 2. P3M3 Process Areas

P3M3 Process Area	Intent
Organizational Governance	Looks at how delivery is aligned to the strategic direction of the organization.
Management Control	Assesses the level to which management is providing direction.
Benefits Management	Ensures that desired outcomes are defined, measurable and delivered.
Risk Management	Ensures opportunities and threats are systematically managed.
Stakeholder Management	Addresses the effective use of communications channels.
Finance Management	Ensures that costs are captured, evaluated and managed.
Resource Management	Addresses processes to manage all resources including human resources, supplies, information, tools and teams.

3.2 Gap/Redundancy Analysis

A gap/redundancy analysis provides a good approach to help ensure migration plans are thorough (no gaps or shortfalls) and optimal (no redundancies or duplications). Gaps and redundancies may cause implementation or operational problems, increase costs, delay implementation, or generally result in a sub-optimal or non-responsive solution. The analysis process compares the current "As Is" and proposed "To Be" environments to identify what can remain and what needs to be added, changed, replaced, or deleted. Maximizing the use of existing processes, technology, governance, etc., takes advantage of user familiarity and will likely result in savings in implementation time and resources, as well as increasing likelihood of success through user familiarity with the IT services. However, significant changes to the IT environment will likely necessitate a great deal of movement away from the "As Is."

This type of analysis helps to identify changes that need to be made, which helps lay out a transition strategy and plan on how to migrate to the "To Be." The general steps to accomplish the analysis are listed below.

- **"As Is" Architecture**. Identify the current environment, or if it is already identified and documented, validate the accuracy (this information constitutes the "As-Is" architecture). Capturing "As Is" issues is also valuable to ensure they are addressed in the planning process.

- **"To Be" Architecture.** Determine the new environment, or "To Be" end state, which can then be used to determine impacts that a transition plan must address. For example, if the migration and follow-on IT operations will move from an internal Government-operated data center to an external contractor-operated cloud environment, then organization, processes, and governance will likely be impacted as described below:

    - **Organization.** Government roles and responsibilities will change from focusing on data center operations and service delivery to focusing on monitoring the performance of the contractor and delivered services. This new focus will change organizational roles, responsibilities, and likely structure, manpower qualifications and needs, and organizational culture.

    - **Processes.** Many of the Government-run processes will become obsolete as roles and responsibilities move to the contractor, and new ones will be required for the contract oversight.

    - **Governance.**[8] Changes in governance such as including directives, instructions, and operating procedures will be required to reflect the change in organization and processes described above.

- **Gap/Redundancy Analysis.** Identify the difference (gaps) between the "As-Is" and the "To-Be," as well as any overlapping or duplicative activities. This analysis will determine what can/should remain, what needs to be changed, and where planning efforts need to be dedicated to plan for the changes. Rationale for deciding what should remain and what should go is based on a business case analysis that factors in mission needs, benefits, costs, and time to migrate.

3.3 Analysis of Alternatives (AoA)

Throughout the lifecycle of a given project, leadership will make key decisions related to requirements (e.g., user and technical performance requirements) and solutions (e.g., cloud deployment model options such as public, private, or hybrid clouds).[9] Decisions will drive the cost, schedule, and performance of the project, and they must balance cost versus benefits.

[8] The MITRE Systems Engineering Guide defines Governance as: "… the responsibilities, structures, and processes by which organizations are directed and controlled."

[9] NIST Special Publication 500-292, *NIST Cloud Computing Reference Architecture*, September 2011, Section 1.2.

An objective, data-driven AoA methodology that supports such decision making can be very useful in evaluating Courses of Action (COAs), and in selecting and defending a given decision. There are a variety of ways to conduct an AoA. Attachment 1 to this document describes one approach as implemented in an MITRE-developed Excel-based tool that can be used to conduct an AoA. Attachment 2 provides a cloud-based example of its use.

The basic premise of the AoA approach described in the attachments is to evaluate various alternatives against defined and weighted cost, schedule, and performance criteria and standards. Scoring how well each alternative meets a given criterion and standard, multiplying that score by the weight, and summing these products across all criteria, generates an overall score for each alternative. The alternative with the highest score is the one that best meets the criteria.[10]

3.4 Plan of Actions and Milestones (POA&M)

When the WBS decomposition, gap/redundancy analysis, and any required AoAs are completed, the planners should understand the direction to proceed including what processes, technology, governance, and organizational construct will remain and what needs to be changed, replaced, or deleted. Additionally, they will have identified the specific actions that need to be taken based on the WBS decomposition. Then, lead organizations, accountable/responsible personnel, and dates can be assigned to each action to create a POA&M, or schedule. The POA&M provides a method and a documented plan to guide and manage the migration, a common approach to share across the migration team and stakeholders, and a means to track status.

4. Planning Considerations

When developing migration plans, the "devil is in the details." Critical planning factors can easily be overlooked. This section focuses on using a WBS to identify the broad factors that should be considered in WBS decomposition and in laying out a POA&M to help in "drilling down" to the details (the WBS breakdowns that are shown in Figures 3 and 4 are based on the example shown in Figure 2).

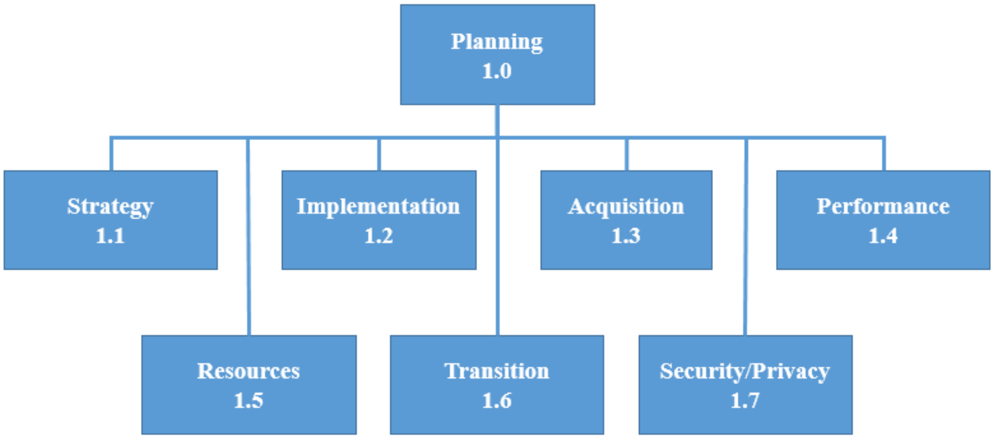


Figure 3. Planning WBS

[10] This methodology is a based on the Kepner-Tregoe decision making process.

Some of the factors may not be applicable to a given project, but considering their applicability and consciously deciding what is or is not relevant helps to reduce overall risk by ensuring a wide range of potential impacting factors are considered.

Based on Figure 3, the following decomposition of planning identifies broad, early planning considerations and highlights some of the key factors/questions that should be considered during initial planning for migration to the new environment. Attachment 3 provides a checklist that summarizes the actions discussed in this Section as well as those in the sections on processes, technology, data, governance, and facilities.

4.1 Strategy (WBS 1.1)

Identify the intended use and requirements, the broad strategy, and the architectural concepts for how cloud services will be delivered:

- Identify what cloud services (SaaS, PaaS, and/or IaaS) and data will be provided.
- Establish from where the services will be provided.
  - In-house data center (on premise) – organically owned and operated by the organization.
  - In-house data center (on premise) – owned and operated by a third party (contractor).
  - External data center (off premise)– outsourced to a federal cloud provider.
  - External data center (off premise)– outsourced to a commercial cloud provider.
- Define what cloud deployment model will be used:[11]
  - Public cloud – available for use by the general public and located on the premises of the cloud provider.
  - Community cloud – exclusively used by a broad community of customers from organizations that share common concerns (e.g., missions, security, policy, compliance guidelines, etc.). This cloud might be located on the premises of the customer or the cloud provider.
  - Private cloud – the cloud infrastructure is dedicated to a specific community of customers. It may be located on the premises of the customer or the cloud provider.
  - Hybrid cloud – a combination of two or more of the above cloud deployment models – public, community, or private.

[11] NIST Special Publication 500-292, *NIST Cloud Computing Reference Architecture*, September 2011.

4.2 Implementation (WBS 1.2)

Define the migration/implementation approach.

- Establish how the migration will occur. Examples of such approaches include:
    - Conducting a Proof of Concept before committing to further implementation.

    - Full implementation – implement all requirements at once.

    - Phased implementation – implement requirements in incremental phases based on a cost vs benefits vs risk analysis to define the implementation strategy. Phasing strategies may include the following:
        - Implement a set of requirements based on priorities that have an immediate operational impact and are achievable in the specified time (i.e., don't bite off more than can be chewed)
        - Migrate low risk capabilities first to learn lessons and refine plans for future increments.
        - Implement requirements in an evolutionary manner in which solutions are implemented, evaluated, and improved on incrementally ("build a little, test a little").

- Identify the framework to be used, and tailor it to the specific project. In the case of a WBS, decompose it to the level where specific actions are defined.

- Develop the POA&M.
    - Complete the WBS down to the action item level to include identifying action officers (leads) and target completion dates for each item.
    - Identify dependencies between actions items.
    - Coordinate/staff the plans and POA&M with the supported and supporting organizations.
    - Baseline the planning document and control changes to it.

- Risk management/mitigation.
    - Risk Identification.
        - Identify actual and possible implementation risks that may adversely impact (or are impacting) implementation, and lay out a mitigation strategy for them.
            - Consider risks at the cloud provider's and cloud customer's locations as well as the transport (communications) network connecting them. Also, consider risks in integrating new cloud technology with legacy systems, networks, infrastructure, processes, etc.
            - Categorize risks by impact and likelihood to ensure that risks are addressed by priority. Table 3 provides an example of ways to

categorize risks, mapping mission impacts and likelihoods of occurrence to risks.

Table 3. Risk Level Assessment

	Mission Impact				
Likelihood	**Very Low**	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Medium	High	Very High	Very High
High	Low	Medium	Medium	High	Very High
Moderate	Low	Low	Medium	Medium	High
Low	Very Low	Low	Low	Medium	Medium
Very Low	Very Low	Very Low	Low	Low	Low

- Identify operational risks that may adversely impact the capability once it is operational. These risks may be due to natural, technological, or human causes., and may be ubiquitous or geographically dependent. Some are predictable, and some are not. Table 4 identifies notional examples of threats and the impacts they may have on facilities, IT, and staffing/personnel. For a given location, risks can be generated by determining the specific threats to that location (likelihood of occurrence) and the specific impact those threats would have on the mission.

Table 4. Threats and Impacts

		Chemical/Biological/ Radiological attack	Conventional attack	Cyber attack	Earthquakes	Fire	Nuclear attack	Nuclear plant meltdown	Pandemic	Snow/Ice/Cold	Terrorism	Tornado	Tsunami/Flood	Typhoon/Hurricane	Volcano/Ash
Category	**Impact**	**Threat**													
All	CIKR single points of failure			X				X							
Facility	Facility Loss		X		X	X	X	X		X	X	X		X	X
Facility	HVAC Outage		X		X	X	X	X		X	X	X		X	X
Facility	Power Outage		X		X	X	X	X		X	X	X		X	
IT	Cyber			X				X							
IT	Data Center Access - External			X				X							
IT	Data Center Outage - Local		X	X	X	X	X	X		X	X	X		X	X
IT	Information Loss/Compromise		X	X	X	X	X	X		X	X	X		X	X
IT	Infrastructure/Servers/Storage Outage		X	X	X	X	X	X		X	X	X		X	X
IT	Network Outage - externaL			X				X							
IT	Network Outage - local		X	X	X	X	X	X			X	X		X	
IT	Systems Outage		X	X	X	X	X	X			X	X	X	X	X
Manning	Manning loss/reduction	X	X		X		X	X	X						

- Risk Mitigation.
  - Develop risk mitigation strategies for both implementation and operational risks.

        - Determine testing requirements to ensure the new capabilities are operating as planned/needed.

    - Determine the need for availability and reliability standards, which drive the following considerations to minimize risks and provide resiliency (the ability to recover from issues):
        - Need for redundancy of equipment and/or communications paths (networks).
        - A COOP or DR plan and possibly an alternative site in case of long term or catastrophic failure.

    - Track these risks in a documented Risk Registry that identifies the risks, priorities, mitigation strategies, responsible office(s), dates for resolution, level of risk, and status.

    - Consider a fall back plan to restore services to their original state in case of implementation failure.

4.3 Acquisition (WBS 1.3)

Involve acquisition experts and contract officers early to help define the contract and acquisition strategy. Factors for consideration include the following.

- For work that will be contracted out:
    - Define the type of contract that will be used for contractor-provided support (e.g., cost plus, firm fixed price, time and materials, performance based, etc.).

    - Determine the type of contract documents and requirement specifications needed such as Statement of Work (SOW), Statement of Objectives (SOO), or Project Work Statement (PWS), as well as associated strategic plans and requirements documents.

    - Consider using existing Government contracts, such as with General Services Administration (GSA) or other federal organizations that have contracts for cloud providers, Indefinite Delivery/Indefinite Quantity (ID/IQ) for equipment/service acquisition, etc.

- Determine requirements for acquiring, upgrading, replacing, or eliminating equipment, software, communications infrastructure, etc. A gap/redundancy analysis can help with this.

- Where possible, leverage open, vendor-neutral standards to provide open competition and avoid becoming locked in to a specific vendor.

4.4 Performance (WBS 1.4)

Establish an approach to performance management/measurement.

- Define the expected/required Quality of Service (QoS) metrics in the form of:
  - SLAs describing the expectations for how services will be delivered to the customer (e.g., reliability, availability, and maintainability requirements; incident response times; etc.).
  - Operating Level Agreements (OLAs) describing the expectations for how the service delivery organization will work with supporting organizations.

- Identify:
  - Specific performance metrics to be captured.
  - Minimum acceptable threshold values and the targets values.
  - How they will be captured (i.e., the tools to capture them, and how the tool will need to be configured).
  - How and when they will be reported.

4.5 Resources (WBS 1.5)

Plan for and acquire the necessary financial and staffing resources to cover the initial acquisition and implementations costs as well as life cycle sustainment costs.

- Identified estimated funding required to cover:
  - Acquisition costs.
    - Data center hardware (infrastructure, storage, services, etc.).
    - Software (applications, licensing, etc.).
    - Networking hardware (routers, switches, etc.).
    - Transport costs.
    - Support costs (logistics, training, manpower/personnel).
  - Contract costs.
  - Life cycle operations and sustainment costs.
    - O&M costs.
    - Manpower/personnel.
    - Logistics.
    - Training.
    - Software acquisition or licensing fees.
    - Life cycle replacement.
    - Facility requirements (e.g., power, air conditioning, cabling, floor space).

- Identify new or changed staffing requirements to support the migration and follow-on O&M. This should address both numbers and skill sets.

- Request the necessary funding and staffing using the organization's internal resourcing processes. Funding requests should be submitted as early as possible to maximize the likelihood of approval.

4.6 Transition (WBS 1.6)

Identify activities required to transition from the current "As Is" to the new "To Be" cloud environment.

- Establish a mechanism to identify and track completion of transition activities.
- Review/update the relevant processes and governance.
- Establish training requirements for new technologies, tools, processes, governance, etc.
- Establish/update staffing requirements if any changes.
- Prepare facilities for new equipment or staff, and ensure the facilities can handle any changes that impact the physical structure (e.g., power, air conditioning, cabling, etc.)
- Over-communicate transition events with supported and supporting organizations.
- At the time of transition, arrange for turnover of key materials such as passwords.

4.7 Security/Privacy (WBS 1.7)

Identify and plan for security and privacy related standards and activities.

- Ensure personnel providing support have the proper security or organizational suitability/fitness clearances, and factor in lead time for acquiring such clearances.
- Define and implement appropriate security controls at both the cloud provider and cloud consumer locations
- Identify cloud security standards, framework, and security/privacy best practices, such as those developed by the Cloud Security Alliance.[12]
- Ensure certification, accreditation, or other operating authorization actions are planned and scheduled, and necessary authorizations to operate will be in place on time.

5. Processes

A process can be defined as: "…a structured set of activities designed to accomplish a specific objective."[13] As new processes are established to support the cloud-based data center consolidation project, or as old ones are updated, they must be:

- Defined and documented in the form of governance and/or standard operating procedures, and placed under a change control process/mechanism.

- Managed to ensure they are clearly defined, understood by the personnel using them (with training as needed), current (modified as needed), baselined, controlled, repeatable, and followed.

- Consistently applied and repeatable regardless of who is executing them or from where.

- Optimized to ensure they are effective, efficient, and aligned to the organization's mission.

[12] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*, 2017.
[13] DESMF Executive Summary.

The ITIL processes listed in Table 5 provide examples of high level processes that should be considered for inclusion in the baseline set of processes. [14]

Table 5. Processes WBS

ITIL Category	ITIL Processes
2.1 Service Strategy	Strategy Management
	Service Portfolio Management
	Financial Management
	Demand Management
	Business Relationship Management
2.2 Service Design	Design Coordination
	Service Catalog Management
	Service Level Management
	Availability Management
	Capacity Management
	IT Service Continuity Management
	Information Security Management
	Supplier Management
2.3 Service Transition	Transition Planning and Support
	Change Management
	Service Asset and Configuration Management
	Release and Deployment Management
	Service Validation and Testing
	Change Evaluation
	Knowledge Management
2.4 Service Operation	Event Management
	Incident Management
	Request Fulfilment
	Problem Management
	Access Management
	Common Service Operations Activities
2.5 Continual Service Improvement	Seven-step Improvement Process
	Service Measurement
	Service Reporting

To identify needed changes to existing processes, the gap/redundancy analysis approach described in Section 4.2 is applicable.

- Identify the current set of processes in place (the "As-Is").

[14] *An Introductory Overview of ITIL® 2011*, The IT Service Management Forum.

- Identify the processes needed to support the new cloud-based architecture (the “To-Be”). The list of ITIL processes listed in Table 5 can serve as a good starting point.

- Compare the two sets of processes to identify needed changes/updates, additions and deletions, keeping in mind the process characteristics described above. This activity will yield a new baselined list of processes which should be properly documented and managed (including change control mechanisms).

Once the new baselined list is established:

- Develop, document, and test the new or amended processes to ensure they meet their intended goals and do not cause any unintended consequences.

- Eliminate processes no longer needed.

- Identify metrics to measure process performance, and any required process management/monitoring tool changes – additions, deletions, and/or re-configurations.

- Notify personnel of changes and provide training as required.

- Control changes to these processes.

- Periodically review processes to ensure they remain current and relevant.

As an example of processes that may need changing, elimination, or additions, if data center operations or cloud services will change to contractor- versus Government-provided, then the revised roles and responsibilities for the affected processes need to be defined. For example, Government personnel may no longer perform O&M responsibilities but instead may serve in more of a Quality Assurance (QA)/ contract monitoring role. Therefore, the Government O&M processes may be eliminated and the QA processes added or amended.

6. Technology

Technology enables the people and processes to accomplish the mission. For the purposes of this paper, it is categorized as shown in Figure 4 below:

- **Hardware**. This refers to the physical assets (infrastructure) required to provide the necessary services (as well as the embedded software necessary to manage/control these assets). It includes servers, storage, and end user devices such as workstations, printers, etc.

- **Software.** This refers to the applications needed to support customer requirements to include;

- General purpose "front office" (customer-facing) software such as office automation tools or commercial software
- "Back office" (non-customer-facing) software such as operating systems or infrastructure performance monitoring tools.
- Legacy systems or applications that support specific mission/functional requirements. If they will be migrated to the cloud, they may need tailoring to run, or run optimally.

- **Transport.** This refers to the transport mechanisms (e.g., network routers, switches, cabling, etc.) that connect the supported organization both with the cloud services (e.g., Wide Area Networks) and internally to the organization (Local Area Networks).

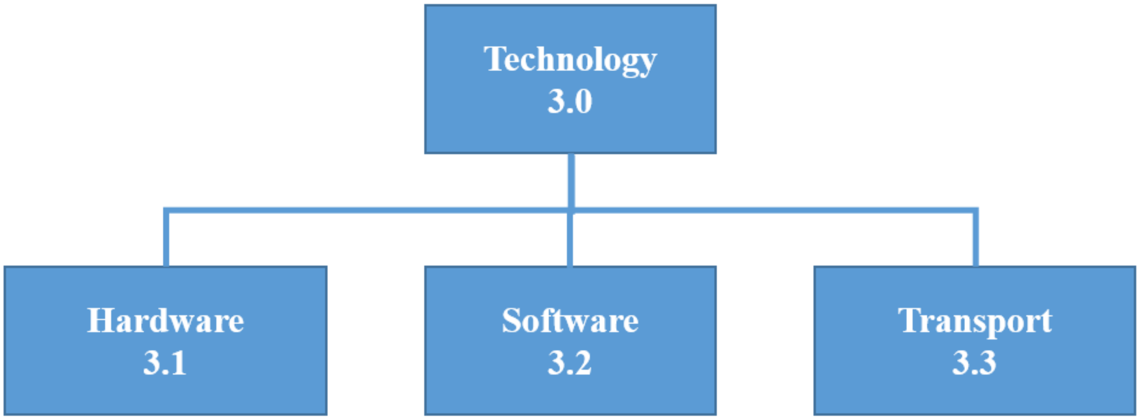


Figure 4. Technology WBS

Considerations for technology planning include the following:

- Ensure sufficient capacity for current and projected requirements with some amount of extra capacity for unforeseen growth.

- Leverage the strengths/benefits of cloud computing to include:
  - High availability, reliability, and resiliency of services. This includes developing COOP/DR strategies.
  - Agility (the ability to quickly respond to future growth, reductions, other requirements changes, or new technologies).
  - Scalability/Elasticity (the ability to adapt to growth or reduction in needed services)
  - Security to include data in transport and data at rest.

Given the decision to migrate and the architecture to be implemented, the project manager should determine what changes need to be made to the baseline – what technology and applications will be needed to support requirements under the new architecture, what should remain locally, and what can be eliminated, reutilized elsewhere, or turned in/decommissioned. Broad actions include the following:

- Identify the current technology/applications in place (the “As-Is” technology/application baseline).

- Identify the technology/applications needed to support the new cloud-based architecture (the “To-Be” baseline) that falls within the auspices of the supported organization (for example, an external cloud provider will be responsible for the equipment within the cloud, not the supported organization).

- Compare the “As-Is” and “To-Be” baselines to identify needed changes/updates, additions and deletions, and document these in a centrally managed and controlled Configuration Management Data Base (CMDB).
    - Consider applications that may need to be re-written, replaced, or decommissioned for the cloud environment.
    - Base the rationale for deciding how to address applications on a business case analysis factoring in mission needs, benefits, costs, and time to implement a given solution.

- Initiate acquisition efforts for new technology (as discussed in Section 5.3) allowing sufficient front-end time to acquire the items.

- Update technology licensing as required.

- Eliminate or turn in technology that is no longer needed.

Regardless of where the service is provided from, ensure the performance of the supporting technology can be measured and managed to achieve the levels of service necessary for users to accomplish their mission or achieve their business goals. Measurement/management tools may be provided by the Cloud Service Provider (CSP) or they may come from the using organization. Either way, leveraging existing tools could reduce costs, so a gap/redundancy analysis should be accomplished to determine what tools can be used. The following describes an approach to accomplishing this analysis:

- Identify services critical to mission/business accomplishment. Define performance requirements and associated metrics for those services. These typically take the form of SLAs/OLAs that describe the required levels of performance (e.g., “the network shall be available 99.9% of the time”).

- Identify monitoring tools available within the organization.

- Compare the required performance metrics against the capabilities of the available tools to capture those metrics and determine gaps and redundancies.

- Use the identified gaps and redundancies to determine which tools are needed, which can be eliminated, and if additional tools are required.

- Establish reporting mechanisms identifying what metrics will be presented to leadership as well as how and how often they will be presented, and who will provide them.

7. Data

With respect to data migration to the cloud, three key areas must be addressed:

- Initial movement of the data stored in the data center to the cloud environment.

- Transport of data between customer locations and the cloud and storage during normal operations.

- Ownership of the data.

Planning considerations for the initial movement of the data to the cloud include the following:

- The organization must plan for how data will be moved to the cloud. It could be migrated physically (e.g., moving storage devices) or across a network. In the latter case, planners must ensure and/or acquire sufficient bandwidth to migrate the data to the cloud within any required time limits. Therefore, planning for adequate bandwidth must be accomplished early enough to ensure sufficient availability when required.

- Data storage in the cloud must be assessed to ensure sufficient capacity "on arrival" with additional capacity for future growth.

- Data should be validated "on arrival" to confirm accuracy and completeness in the transport process.

- Applications must be assessed for compatibility with data before migration to ensure operational use after migration.

- Plans should be developed in accordance with organizational governance to ensure the security of the data in transit. This include establishing security controls, processes for how to handle and protect the data at both ends, mechanisms to encrypt the data in transit, and plans on how to respond to accidental or intentional loss or other cyber threats.

To ensure adequate transport of data once "normal" operations are in place, the organization needs to consider:

- Bandwidth and capacity management for transport and storage to ensure adequate support for current and future projected requirements (with some capacity for unknown/unforeseen requirements).

- Backup plans to ensure availability and access of data. This may include a separate continuity plan and/or an alternate storage or COOP site.

- Duplicate/alternate communications paths between customer locations, the CSP, and possibly a COOP site to ensure redundancy of transport.

- Plans to ensure the security of the data both in transit and at rest.

Ownership of the data needs to be considered. If data resides on a CSP's servers, who owns and controls the data? What happens to the data when the service contract expires or is terminated? What happens if the CSP goes out of business? Data stored in the cloud could include intellectual property, mission or business-specific data, technical or scientific data. The legal implications of this issue are beyond the scope of this paper, other than to identify the need to address the issue with the appropriate acquisition, contracting, or legal offices.

8. Governance

As previously stated, the publicly releasable MITRE Systems Engineering Guide defines Governance as: "… the responsibilities, structures, and processes by which organizations are directed and controlled."

Therefore, Governance refers to how an IT organization places management/control structure around its IT service delivery to ensure business-IT alignment and effective/efficient service delivery. It provides both direction and context for how an organization plans for, acquires, operates, maintains, secures, and terminates its use of IT in support of providing services to a customer in support of its mission or business goals. It also supports and provides mechanisms for resource allocation and investment decisions.

Governance can take the form of policies, directives, instructions, frameworks, defined processes, standard operating procedures, security controls, etc. To be effective, they must be documented with a mechanism in place (e.g., auditing) to ensure they are followed.

Migration to a new cloud based architecture will impact some (perhaps much) of the existing governance. Therefore, the implementing organization should make sure they know what their current governance baseline is, determine what changes need to be made, and then establish a migration plan. The gap/redundancy analysis approach described in Section 4.2 is applicable.

To identify needed changes to existing processes, the gap analysis consists of the following steps.

- Identify the current governance in place (the "As-Is").

- Identify governance needed to support the new cloud-based architecture (the “To-Be”).

- Compare the two sets of processes to identify needed changes/updates, additions and deletions, keeping in mind the process characteristics described above. This activity will yield a new baselined list of governances, which should be properly documented, managed (including change control mechanisms), and promulgated.

Once the new baselined list is established:

- Develop, document, and coordinate new or amended governance with the stakeholders (users and supporting staff) to ensure it meets the intended goals and does not cause any unintended consequences.

- Eliminate governance and related processes no longer needed.

- Notify personnel of changes and provide training as required.

- Control changes to the governance once it has been approved through a formal organization change control process (e.g., a Change Control Board).

- Periodically review governance to ensure it remains current and relevant.

9. Facilities

Facilities preparations need to be factored into the planning to assure that sufficient capacity is planned in and/or no-longer-needed space can be freed up, depending on the “To Be” architecture/environment. Planning factors may include:

- Heating, Ventilation, and Air Conditioning (HVAC) capacity.
- Power, including separation of components to minimize risk in case of power loss.
- Floor space (current and projected growth/reduction).
- Facility security and access control.
- Physical separation of components for safety/security reasons.
- Associated funding.
- The need for a COOP/DR facility.

Usually, the IT organization is not responsible for facility O&M. In those circumstances, the IT and facility organizations need to ensure IT and facility plans are known, understood, and synchronized.

10. Organizational Impacts

Major architectural changes will greatly impact the structure, roles and responsibilities of the IT organization and its staff. Old roles may disappear and new ones may be created. For example, if the current organization provides the staff to operate and maintain the data center, but the data center services are migrated to an external cloud provider, then the O&M staff will no longer be needed in that capacity; instead, there likely will be an increased need for contractor oversight and QA monitoring. These changes may mean the existing organizational structure and staffing are no longer effective or efficient. Therefore, as part of the upfront planning, organizational leadership needs to determine if organizational change is necessary. If it is, leadership must consider the best way to change the organizational structure and staffing to align with the new mission/environment and changed roles and responsibilities. Some key considerations include:[15]

- **Mission:** align the organization to the mission, not the systems.

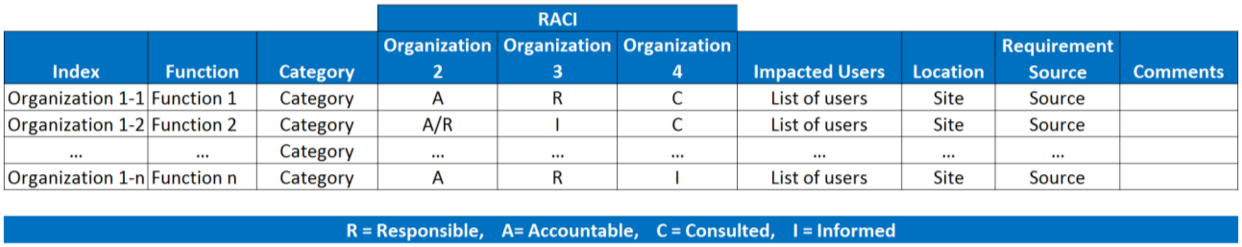
- **Strategy:** ensure the stakeholders (and especially the internal staff) understand the purpose and direction of the change, and how/why it is affecting the organizational structure,

- **Structure:** arrange functions and staff into specific areas of responsibility, and ensure all functions are addressed (particularly focusing on new or changed ones).

- **Authority:** provide the necessary authority to link responsibility with accountability. Document authorities in governance and communicate them across the staff.

- **Relationships:** Identify and describe relationships across the organization. A RACI (Responsible, Accountable, Coordinated, Informed) model[16] may be useful to capture roles and relationships within and between organizational elements. Table 6 shows a notional RACI view of how an organization ("Organization 1") can identify its core functions (indexed as Organization 1-1, 1-2, etc.), and then relate each of them to other organizations (Organizations 2-4) in terms of R, A, C, and/or I relationships.

Table 6. Notional RACI Chart



			RACI						
Index	Function	Category	Organization 2	Organization 3	Organization 4	Impacted Users	Location	Requirement Source	Comments
Organization 1-1	Function 1	Category	A	R	C	List of users	Site	Source	
Organization 1-2	Function 2	Category	A/R	I	C	List of users	Site	Source	
…	…	Category	…	…	…	…	…	…	
Organization 1-n	Function n	Category	A	R	I	List of users	Site	Source	

R = Responsible, A= Accountable, C = Consulted, I = Informed

[15] These considerations are derived from the Burke-Litwin Organization Performance Model (Burke, W. W., 1992, *Organizational Development: A Process of Learning and Changing*, 2nd Edition, Addison-Wesley Publishing Company).
[16] Bob Kantor, CIO, "How to Design a Successful RACI Project Plan," CIO online magazine (http://www.cio.com/article/2395825/project-management/how-to-design-a-successful-raci-project-plan.html)

- **Tasks and Individual Skills:** ensure the stakeholders and staff have the necessary skills, ability, and knowledge to perform in the new environment. Documenting governance and providing training can be a big key to success.

- **Communicate:** keep all stakeholders (users, CSP, technical staff, resource managers, etc.) aware of and involved with direction, status, and issues.

Migration to a CSP can be a major change to an organization, affecting its roles and responsibilities, structure, required staffing and skillsets, image, etc. The size and scope of these changes can have major impacts on an organization's people and its cultural climate leading to turbulence, disruption, uncertainty, fear, and resistance to change among the staff. Keeping them involved and well-informed will help minimize these issues, which increases their comfort level and degree of support, as well as reducing the risk of early departures affecting O&M, customer service, and/or transition activities.

To address the optimal way to introduce these changes, the organization may want to consider bringing in Subject Matter Experts (SMEs) in organizational change management to help define, plan, and implement organizational change. MITRE has SMEs in K81C, Human and Organizational Systems.

11. Summary

The intent of this document is to provide a high-level, management-oriented approach to planning for the migration to a cloud-based architecture. It identifies frameworks to manage the migration, and identifies high-level factors that must be considered and planned for to help ensure success. In short, this document provides a starting point to help federal organizations begin their planning process for migrating to a consolidated, cloud-based data center.

Addressing the planning factors and using the frameworks, "best practices," and tools identified in this paper, offer the potential to greatly increase the quality, timeliness, and success of an organization's planning activities to migrate to a cloud environment. Leveraging this information will more quickly jump start the migration planning process, increase its effectiveness and efficiency, reduce time and resource requirements, and decrease implementation and operational risks. It will also have a beneficial impact on performance, cost, and schedule, and increase the overall probability of success.

Attachment 1. Analysis of Alternatives (AoA) Process

The AoA process described below provides a way to objectively and quantitatively assess potential Courses of Action (COAs) against each other to select the best one. It uses an Excel-based tool to conduct the analysis. This tool has been used for MITRE-conducted AoAs in support of the US Special Operations Command, the Social Security Administration, and the Federal Communications Commission.

Given an objective and an identified set of COAs, this AoA provides a side-by-side comparison of the COAs in terms of their ability to meet specified and weighted cost, schedule, and performance criteria. The assessment process scores each COA by the same set of weighted criteria, and ranks the COAs by the accumulated scores. Figure 5 below depicts the process for assessing the alternatives with more details provided below.

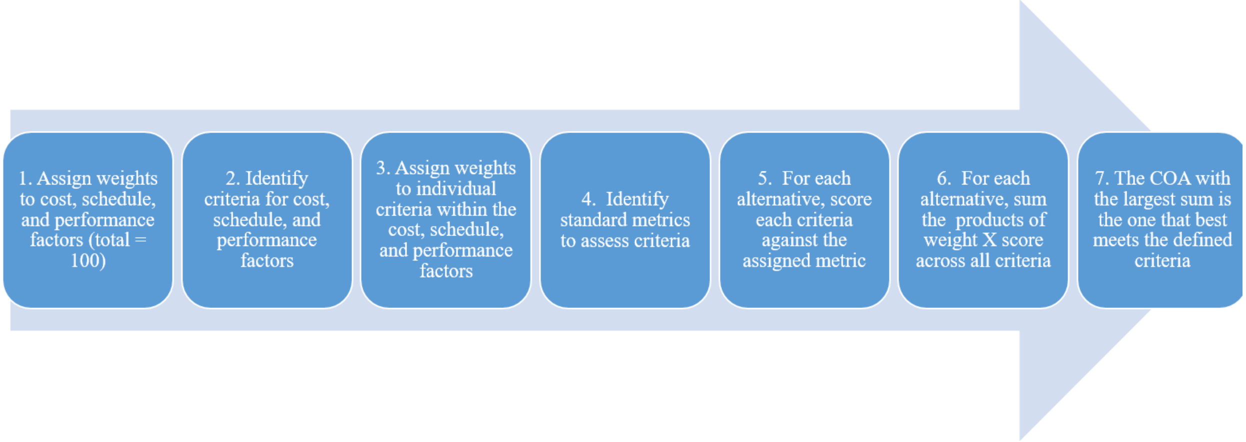

1. Assign weights to cost, schedule, and performance factors (total = 100)
2. Identify criteria for cost, schedule, and performance factors
3. Assign weights to individual criteria within the cost, schedule, and performance factors
4. Identify standard metrics to assess criteria
5. For each alternative, score each criteria against the assigned metric
6. For each alternative, sum the products of weight X score across all criteria
7. The COA with the largest sum is the one that best meets the defined criteria

Figure 5. Assessment Process

The following provides a step-by step description of the AoA process.

1. Assign weights to the broad categories of performance, cost, and schedule. Using a scale of 100 points divided among the three categories is an intuitive way to identify the relative importance of each. For example, if performance is more important than cost, which is more important than schedule, the 100 points might be allocated with 50 going to performance, 30 going to cost, and 20 going to schedule.

2. Identify assessment criteria within each of the broad categories. For example, costs might be broken down by acquisition, annual O&M, or personnel costs. Performance might be broken down by technical criteria, service quality, or transition risks. Schedule might be broken down by the likelihood of meeting specified dates.

3. Assign weights to each of the criteria such that the sum of the weights within the broad category adds up to the number of points allocated to that category. For example, if performance is allocated at 50 points and has five equally-weighted criteria defined, then each criterion is weighted at 10 points. If the criteria are not equally weighted, then they

must add up to 50 within the performance category. For category or criteria weights, the Excel tool has the flexibility to quickly and easily change these weights (or add new criteria) for the purposes of a sensitivity analysis or to see the impact of other weight allocations. It also provides a means to catch and highlight math errors associated with miscalculating criteria weights.

4. Identify metrics that will be used to measure how well a COA meets each criterion. In some cases, the assessments will be objective (e.g., the COA meets/does not meet the criteria), but in other cases they might be more subjective or relative (e.g., COA 1 meets the criteria better than COA 2). The metric should range between 0 and 1, where 0 does not meet the criteria, 1 does meet it, and scores in-between provide a means to establish how well it meets the criteria. Examples of such metrics are listed in Table 7 below.

Table 7. Assessment Criteria and Associated Metrics (Examples)

Criteria	Metric
The COA meets the requirements (absolute)	Y = 1, N = 0
The COA meets the requirements (relative)	Fully meets the requirement = 1 Meets most of the requirements = 0.75 Meets some of the requirements = 0.5 Meets a few of the requirements = 0.25 Meets none of the requirements = 0
The quantitative degree to which the COA meets the requirement	≥ 90% = 1 80 – 89% = 0.67 71 – 79% = 0.33 ≤ 70%= 0
The likelihood of the COA meeting the requirements	High probability = 1 Moderate probability = 0.5 Low probability of meeting requirements = 0.25 Will not meet requirements = 0
Costs of the COA (e.g., acquisition, annual, lifecycle costs, etc.)	COA is assigned a point value based on the range of cost differences between the COAs
Comparing capabilities to a baseline value (e.g., an "as is" COA), the COA:	Provides many more capabilities = 1 Provides more capabilities = 0.75 Provides equal capabilities = 0.5 Provides fewer capabilities = 0.25 Provides far fewer capabilities = 0

Comparing costs to a baseline (when absolute costs are not known), the relative cost of the COA is:	Much less = 1
	Less = 0.75
	Equal = 0.5
	More = 0.25
	Much more = 0

Pair-wise comparison - each COA is individually compared against the others in terms of which best meets the criteria	Best meets the criteria = 1 Least meets the criteria = 0 Equally meets the criteria = 0.5
Complexity or risk of solution	High complexity or risk= 0 Moderate complexity or risk = 0.5 Low complexity or risk = 1

5. Each COA is then assessed against each criterion based on the defined metric, and the score for that assessment equals the product of the weight times the assessed metric score. For example, if a criterion for a given COA were weighted at 10 points, and the COA fully met the criteria, it received 10 points -- weight (10) X “met criteria” (1) = 10. The Excel tool does these calculations.

6. For each COA, sum the products of the weights times the scores across all criteria to generate an overall COA score.

7. The COA with the largest overall score is the one that best meets the defined criteria. If two or more COAs are very close in scoring, then the criteria and weights need to be further refined and the AoA conducted again with the new/revised criteria to differentiate between the “tied” COAs.

Documenting the rationale behind the assessment is recommended to help ensure objectivity and to defend the conclusion of the AoA.

This page intentionally left blank.

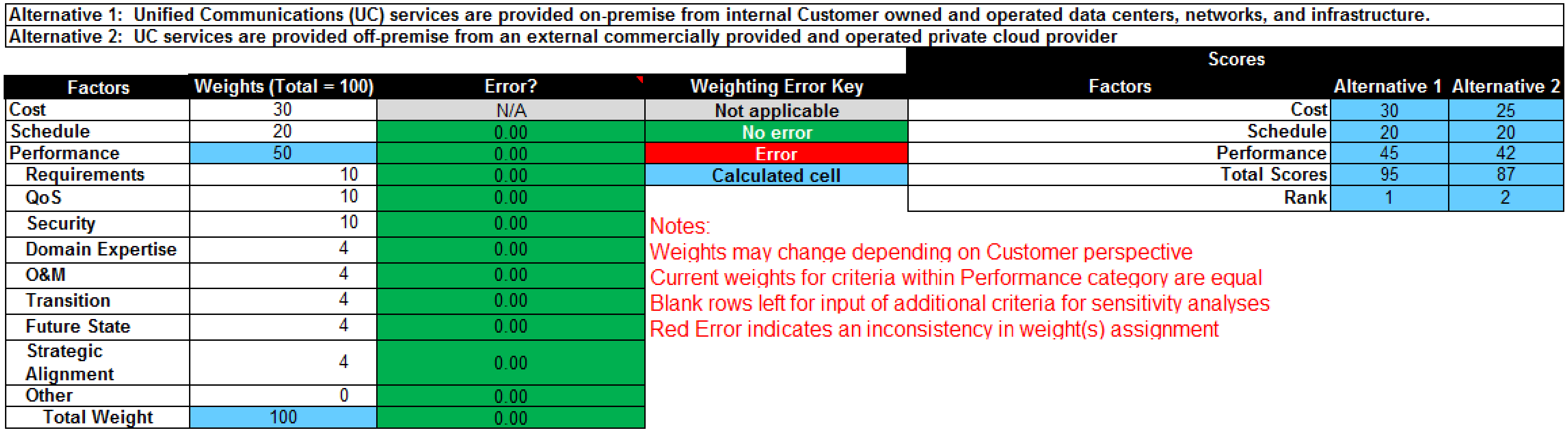
Attachment 2. Analysis of Alternatives (AoA) Example

This Attachment provides a real-world example of the process applied to a MITRE customer, and uses the Excel tool previously mentioned. In this example, the customer is assessing two COAs:

- COA 1: provide services from internally owned and operated data center, networks, and infrastructure
- COA 2: receive services off-premise from an external, commercial cloud service provider

The Excel spreadsheet has four sections – summary and scoring, cost, schedule, and performance.

The first is a summary section which includes the cost, schedule, and performance factors; weights; error column that highlights (in red) errors in the weights; overall scores for cost, schedule, and performance categories; and the ranking of the COAs.



Alternative 1: Unified Communications (UC) services are provided on-premise from internal Customer owned and operated data centers, networks, and infrastructure.
Alternative 2: UC services are provided off-premise from an external commercially provided and operated private cloud provider

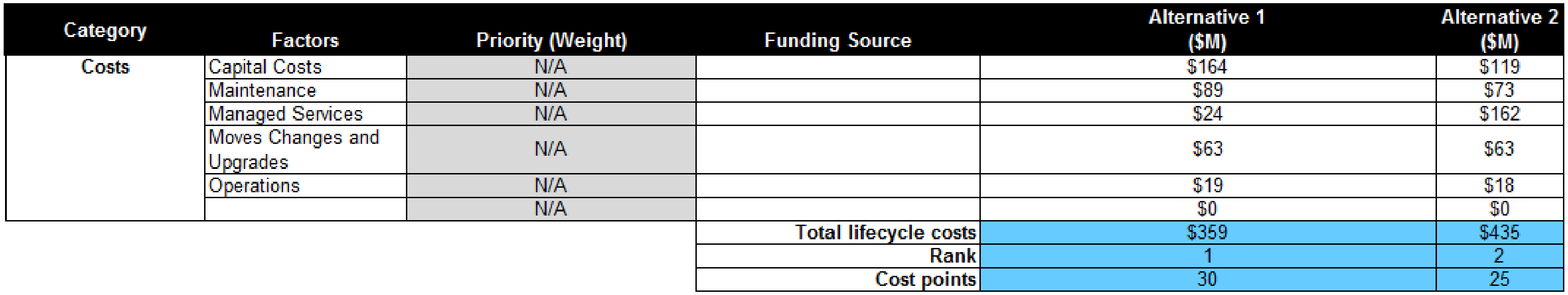
Factors	Weights (Total = 100)	Error?
Cost	30	N/A
Schedule	20	0.00
Performance	50	0.00
Requirements	10	0.00
QoS	10	0.00
Security	10	0.00
Domain Expertise	4	0.00
O&M	4	0.00
Transition	4	0.00
Future State	4	0.00
Strategic Alignment	4	0.00
Other	0	0.00
Total Weight	100	0.00

Weighting Error Key
Not applicable
No error
Error
Calculated cell

	Scores	
Factors	Alternative 1	Alternative 2
Cost	30	25
Schedule	20	20
Performance	45	42
Total Scores	95	87
Rank	1	2

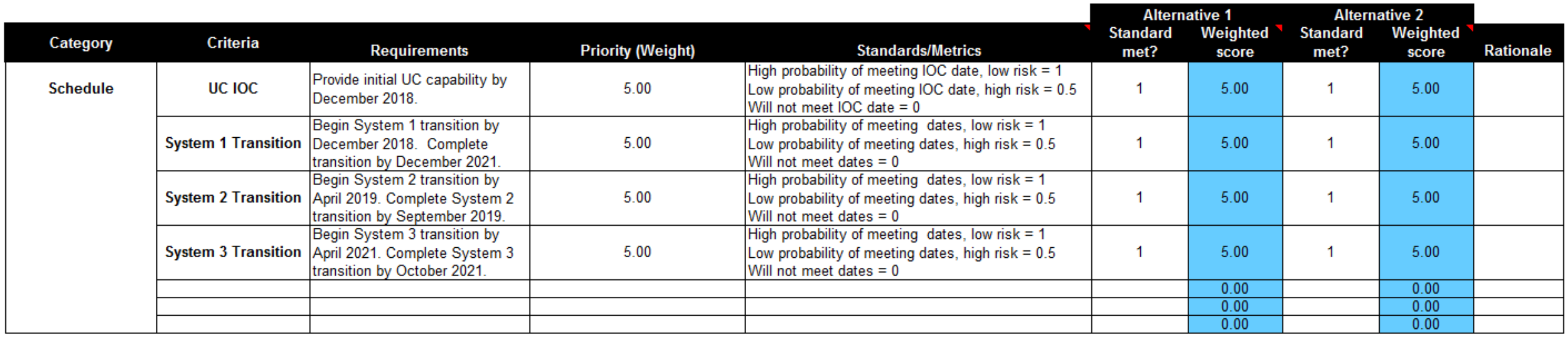
Notes:
Weights may change depending on Customer perspective
Current weights for criteria within Performance category are equal
Blank rows left for input of additional criteria for sensitivity analyses
Red Error indicates an inconsistency in weight(s) assignment

The second section shows the costs categories and values. Note that no weights are assigned since the scoring is based on total costs.



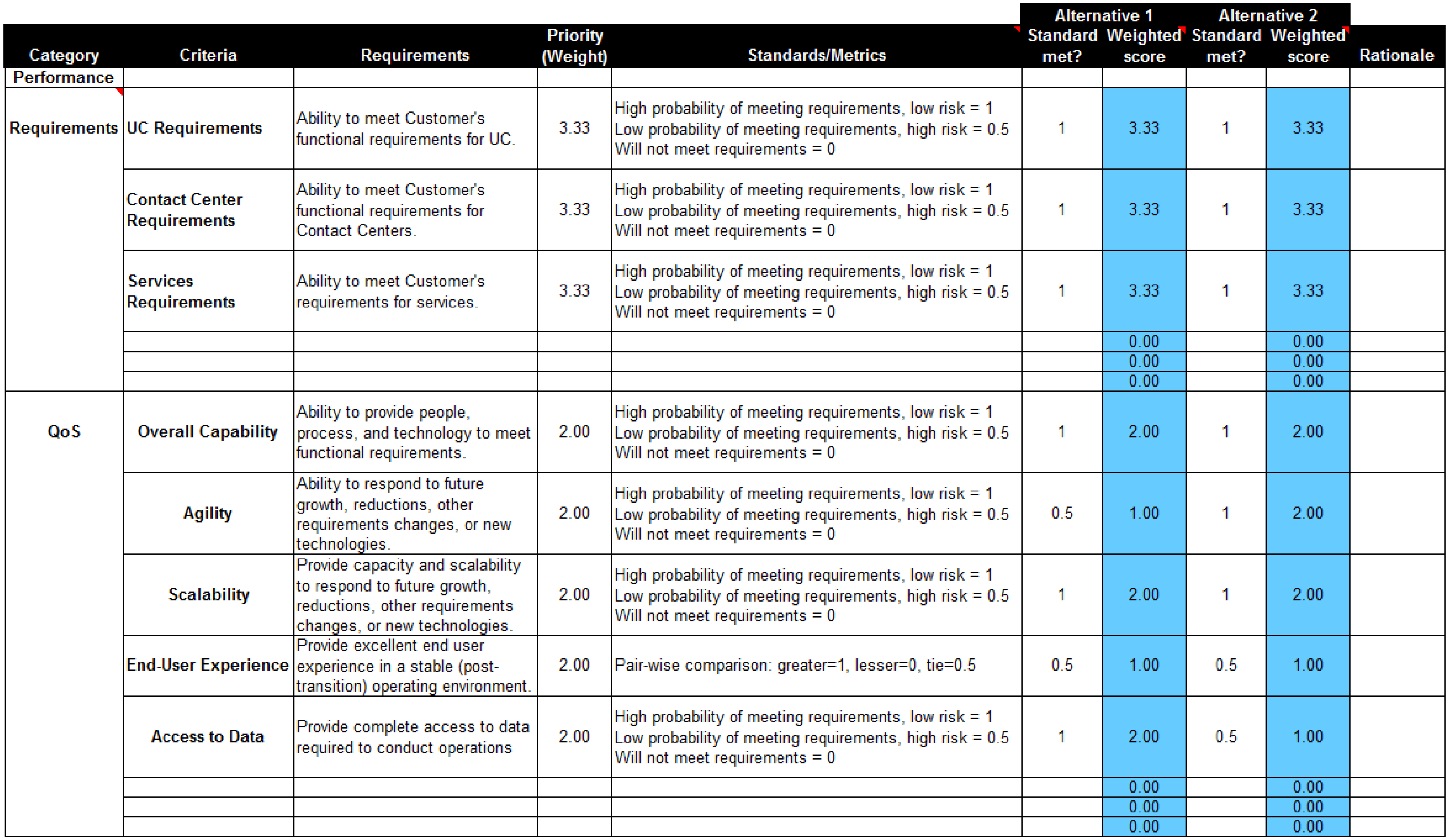
Category	Factors	Priority (Weight)	Funding Source	Alternative 1 ($M)	Alternative 2 ($M)
Costs	Capital Costs	N/A		$164	$119
	Maintenance	N/A		$89	$73
	Managed Services	N/A		$24	$162
	Moves Changes and Upgrades	N/A		$63	$63
	Operations	N/A		$19	$18
		N/A		$0	$0
			Total lifecycle costs	$359	$435
			Rank	1	2
			Cost points	30	25

The third section covers schedule event, specifically, can Systems 1-3 complete their transition in time to meet the UC Initial Operating Capability (IOC) date. The empty criteria rows at the bottom allow for Users to insert additional criteria if desired. In this example, criteria are equally weighted.

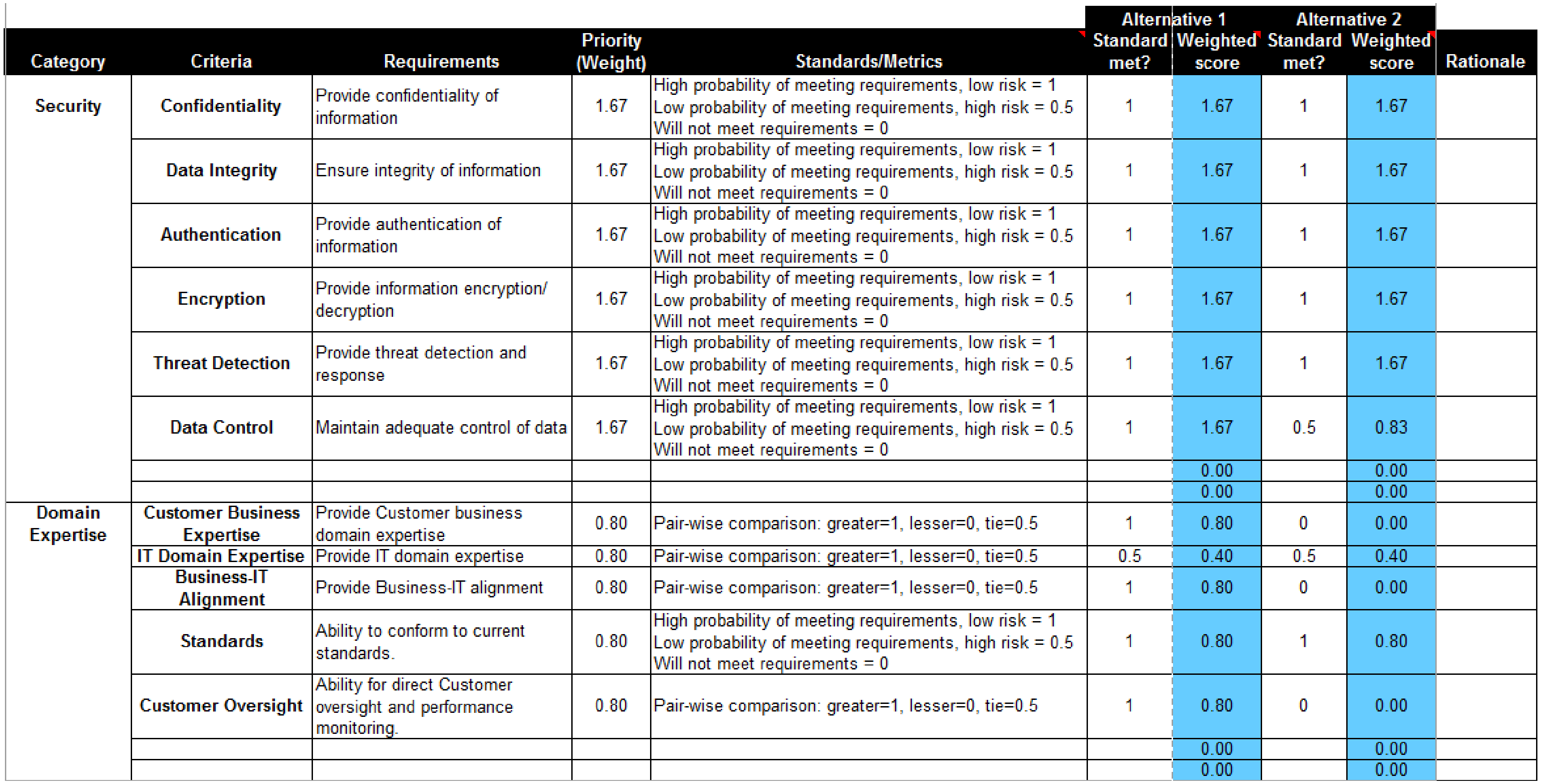


					Alternative 1		Alternative 2		
Category	Criteria	Requirements	Priority (Weight)	Standards/Metrics	Standard met?	Weighted score	Standard met?	Weighted score	Rationale
Schedule	UC IOC	Provide initial UC capability by December 2018.	5.00	High probability of meeting IOC date, low risk = 1 Low probability of meeting IOC date, high risk = 0.5 Will not meet IOC date = 0	1	5.00	1	5.00	
	System 1 Transition	Begin System 1 transition by December 2018. Complete transition by December 2021.	5.00	High probability of meeting dates, low risk = 1 Low probability of meeting dates, high risk = 0.5 Will not meet dates = 0	1	5.00	1	5.00	
	System 2 Transition	Begin System 2 transition by April 2019. Complete System 2 transition by September 2019.	5.00	High probability of meeting dates, low risk = 1 Low probability of meeting dates, high risk = 0.5 Will not meet dates = 0	1	5.00	1	5.00	
	System 3 Transition	Begin System 3 transition by April 2021. Complete System 3 transition by October 2021.	5.00	High probability of meeting dates, low risk = 1 Low probability of meeting dates, high risk = 0.5 Will not meet dates = 0	1	5.00	1	5.00	
						0.00		0.00	
						0.00		0.00	
						0.00		0.00	

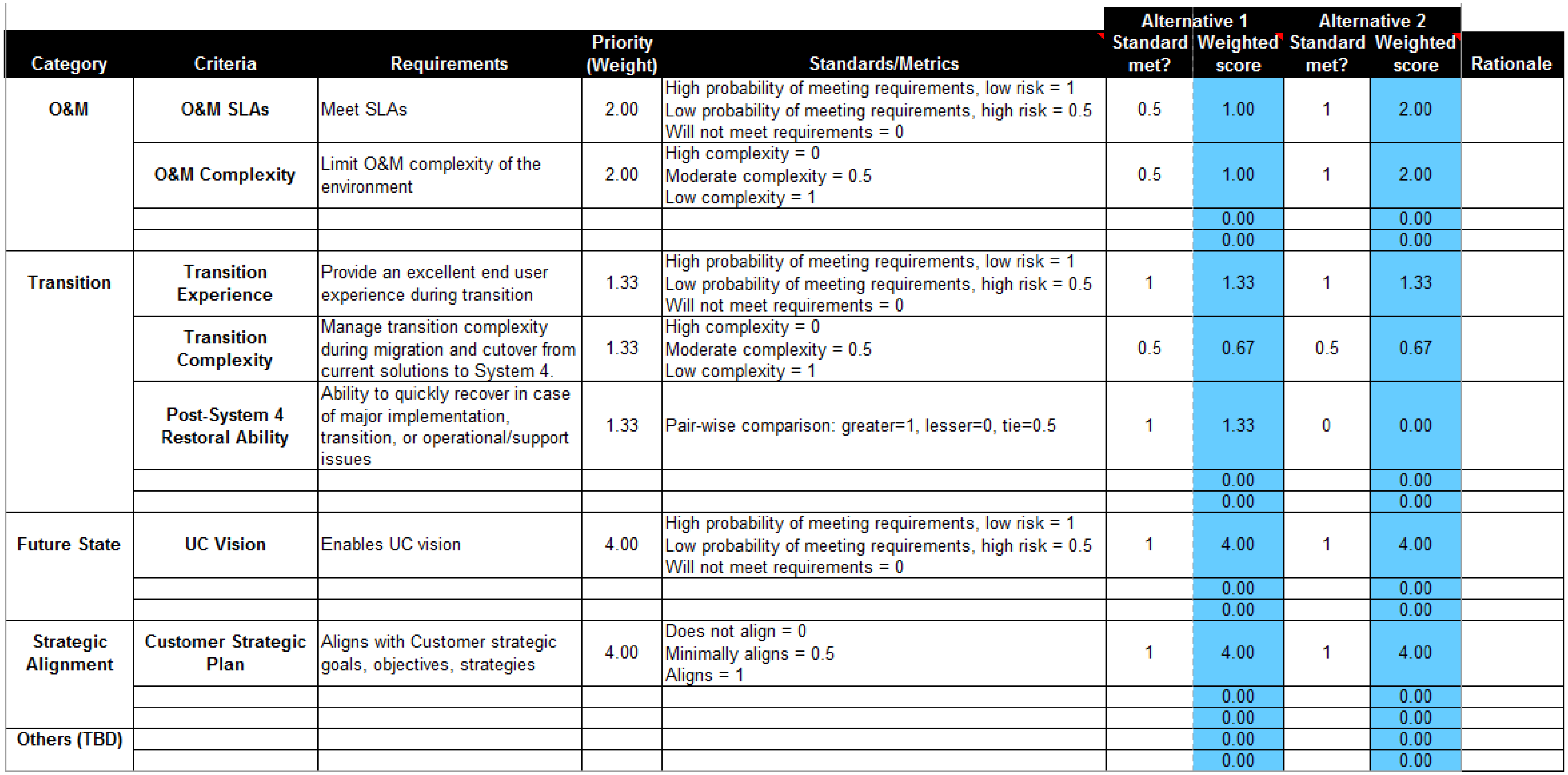
The fourth section covers the performance category, which is subdivided into performance requirements, Quality of Service (QoS), Security, Domain Expertise, O&M, Transition, Future State, Strategic Alignment, and Others. Similar to the schedule section, blank rows allow for additional criteria if identified. In this example, criteria are equally weighted.



					Alternative 1		Alternative 2		
Category	Criteria	Requirements	Priority (Weight)	Standards/Metrics	Standard met?	Weighted score	Standard met?	Weighted score	Rationale
Performance									
Requirements	UC Requirements	Ability to meet Customer's functional requirements for UC.	3.33	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	3.33	1	3.33	
	Contact Center Requirements	Ability to meet Customer's functional requirements for Contact Centers.	3.33	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	3.33	1	3.33	
	Services Requirements	Ability to meet Customer's requirements for services.	3.33	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	3.33	1	3.33	
						0.00		0.00	
						0.00		0.00	
						0.00		0.00	
QoS	Overall Capability	Ability to provide people, process, and technology to meet functional requirements.	2.00	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	2.00	1	2.00	
	Agility	Ability to respond to future growth, reductions, other requirements changes, or new technologies.	2.00	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	0.5	1.00	1	2.00	
	Scalability	Provide capacity and scalability to respond to future growth, reductions, other requirements changes, or new technologies.	2.00	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	2.00	1	2.00	
	End-User Experience	Provide excellent end user experience in a stable (post-transition) operating environment.	2.00	Pair-wise comparison: greater=1, lesser=0, tie=0.5	0.5	1.00	0.5	1.00	
	Access to Data	Provide complete access to data required to conduct operations	2.00	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	2.00	0.5	1.00	
						0.00		0.00	
						0.00		0.00	
						0.00		0.00	



					Alternative 1		Alternative 2		
Category	**Criteria**	**Requirements**	**Priority (Weight)**	**Standards/Metrics**	**Standard met?**	**Weighted score**	**Standard met?**	**Weighted score**	**Rationale**
Security	**Confidentiality**	Provide confidentiality of information	1.67	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	1.67	1	1.67	
	Data Integrity	Ensure integrity of information	1.67	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	1.67	1	1.67	
	Authentication	Provide authentication of information	1.67	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	1.67	1	1.67	
	Encryption	Provide information encryption/ decryption	1.67	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	1.67	1	1.67	
	Threat Detection	Provide threat detection and response	1.67	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	1.67	1	1.67	
	Data Control	Maintain adequate control of data	1.67	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	1.67	0.5	0.83	
						0.00		0.00	
						0.00		0.00	
Domain Expertise	**Customer Business Expertise**	Provide Customer business domain expertise	0.80	Pair-wise comparison: greater=1, lesser=0, tie=0.5	1	0.80	0	0.00	
	IT Domain Expertise	Provide IT domain expertise	0.80	Pair-wise comparison: greater=1, lesser=0, tie=0.5	0.5	0.40	0.5	0.40	
	Business-IT Alignment	Provide Business-IT alignment	0.80	Pair-wise comparison: greater=1, lesser=0, tie=0.5	1	0.80	0	0.00	
	Standards	Ability to conform to current standards.	0.80	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	0.80	1	0.80	
	Customer Oversight	Ability for direct Customer oversight and performance monitoring.	0.80	Pair-wise comparison: greater=1, lesser=0, tie=0.5	1	0.80	0	0.00	
						0.00		0.00	
						0.00		0.00	



					Alternative 1		Alternative 2		
Category	Criteria	Requirements	Priority (Weight)	Standards/Metrics	Standard met?	Weighted score	Standard met?	Weighted score	Rationale
O&M	O&M SLAs	Meet SLAs	2.00	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	0.5	1.00	1	2.00	
	O&M Complexity	Limit O&M complexity of the environment	2.00	High complexity = 0 Moderate complexity = 0.5 Low complexity = 1	0.5	1.00	1	2.00	
						0.00		0.00	
						0.00		0.00	
Transition	Transition Experience	Provide an excellent end user experience during transition	1.33	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	1.33	1	1.33	
	Transition Complexity	Manage transition complexity during migration and cutover from current solutions to System 4.	1.33	High complexity = 0 Moderate complexity = 0.5 Low complexity = 1	0.5	0.67	0.5	0.67	
	Post-System 4 Restoral Ability	Ability to quickly recover in case of major implementation, transition, or operational/support issues	1.33	Pair-wise comparison: greater=1, lesser=0, tie=0.5	1	1.33	0	0.00	
						0.00		0.00	
						0.00		0.00	
Future State	UC Vision	Enables UC vision	4.00	High probability of meeting requirements, low risk = 1 Low probability of meeting requirements, high risk = 0.5 Will not meet requirements = 0	1	4.00	1	4.00	
						0.00		0.00	
						0.00		0.00	
Strategic Alignment	Customer Strategic Plan	Aligns with Customer strategic goals, objectives, strategies	4.00	Does not align = 0 Minimally aligns = 0.5 Aligns = 1	1	4.00	1	4.00	
						0.00		0.00	
						0.00		0.00	
Others (TBD)						0.00		0.00	
						0.00		0.00	

This page intentionally left blank.

Attachment 3. Planning Checklist

This attachment provides a high-level checklist that summarizes the key actions that should be considered in planning a cloud migration project, as described in Sections 5-10. It is indexed using a WBS framework, and links actions where appropriate with the approaches described in Section 4.

Category	WBS Index	Action	Approach	Reference Section
Planning	1.0	Develop migration plan	AoA and gap/ redundancy analyses may be needed during these actions	5
Strategy	1.1	Define migration strategy		5.1
	1.1.1	Identify intended use and requirements		
	1.1.2	Identify broad strategy and architectural concepts		
	1.1.3	Identify what cloud services will be provided		
	1.1.4	Establish from where the services will be provided		
	1.1.5	Define the cloud deployment model		
Implementation approach	1.2	Establish implementation approach	This checklist assumes a WBS framework	5.2
	1.2.1	Identify the framework		
	1.2.2	Decompose the WBS down to the action item level		
	1.2.3	Develop the POA&M	POA&M	
	1.2.3.1	Assign dates and responsible organizations/individual to each action item		
	1.2.3.2	Identify dependencies between the action items		
	1.2.3.3	Coordinate it among the stakeholders for agreement and approval		
	1.2.4	Identify risks and develop strategies to mitigate or avoid them	Risk management	
Acquisition	1.3	Develop acquisition/contracting strategy	Analysis of alternatives and	5.3

Category	WBS Index	Action	Approach	Reference Section
	1.3.1	If contracting, determine strategy and approach	gaps/redundancies may be needed during these actions	
	1.3.2	Determine requirements to acquire, upgrade, replace or eliminate equipment, software, infrastructure, etc.		
Performance	1.4	Establish approach to performance management and measurement		5.4
	1.4.1	Define QoS standards		
	1.4.2	Identify performance measurements (metrics)		
	1.4.3	Define how and when metrics will be captured and reported		
Resources	1.5	Identify resource requirements		5.5
	1.5.1	Funding		
	1.5.1.1	Identify acquisition and contracting costs		
	1.5.1.2	Identify O&M and life cycle sustainment costs		
	1.5.2	Identify new/changed staffing requirements		
	1.5.3	Submit requests for funding/staffing resources		
Transition	1.6	Identify transition activities	A POA&M and a risk registry are examples of such mechanisms	5.6
	1.6.1	Establish mechanism to identify and track transition activities		
	1.6.2	Review existing processes and governance and add, update, or delete as required	Gap/redundancy analysis	
	1.6.3	Establish training requirements based on the changed environment		
	1.6.4	Identify facilities changed needed for the new environment		
	1.6.5	Arrange for turnover of key material at transition		
Security/ Privacy	1.7	Identify/plan for security and privacy standards and activities		5.7

Category	WBS Index	Action	Approach	Reference Section
	1.7.1	Acquire/ensure personnel have necessary clearances		
	1.7.2	Identify cloud security standards, framework, and best practices		
	1.7.3	Acquire necessary authorizations to operate		
Processes	2.0	Identify changes to existing processes	Gap/redundancy analysis	6
	2.1	Identify the "As Is" processes currently in place		
	2.2	Identify the "To Be" processes needed to support the new environment		
	2.3	Compare the "As Is" and "To Be" to identify needed additions, updates, or deletions		
	2.4	Develop and test new/changed processes		
	2.5	Train personnel on these processes		
Technology	3.0	Plan for the integration of new technology		7
	3.1	Hardware		
	3.1.1	Identify the "As Is" hardware baseline currently in place	Gap/redundancy analysis	
	3.1.2	Identify the "To Be" hardware baseline in the new environment, factoring in capacity, availability, reliability, and resiliency requirements		
	3.1.3	Compare the "As Is" and "To Be" to identify needed additions, updates, or deletions		
	3.1.4	Define standards/objectives for availability, reliability and resiliency		
	3.1.5	Initiate acquisition efforts as needed		
	3.1.6	Update licensing as required		

Category	WBS Index	Action	Approach	Reference Section
	3.1.7	Eliminate or turn in technology no longer needed		
	3.2	Software		
	3.2.1	Identify the "As Is" software/systems baseline currently in place	Gap/redundancy analysis	
	3.2.2	Identify the "To Be" software/systems baseline in the new environment, factoring in capacity, availability, reliability, and resiliency requirements		
	3.2.3	Compare the "As Is" and "To Be" to identify needed additions, updates, or deletions		
	3.2.4	Define standards/objectives for availability, reliability and resiliency		
	3.2.5	Initiate acquisition efforts as needed		
	3.2.6	Update licensing as required		
	3.2.7	Eliminate or turn in technology no longer needed		
	3.3	Transport		
	3.3.1	Identify the "As Is" transport baseline currently in place	Gap/redundancy analysis	
	3.3.2	Identify the "To Be" transport baseline in the new environment, factoring in capacity, availability, reliability, and resiliency requirements		
	3.3.3	Compare the "As Is" and "To Be" to identify needed additions, updates, or deletions		
	3.3.4	Define standards/objectives for availability, reliability and resiliency		
	3.3.5	Initiate acquisition efforts as needed		
	3.3.6	Update licensing as required		

Category	WBS Index	Action	Approach	Reference Section
	3.3.7	Eliminate or turn in technology no longer needed		
	3.4	Plan for technology-related COOP/DR strategy and acquisition if needed		
Data	4.0	Data Migration		8
	4.1	Plan for initial movement of data to the cloud environment and validation on arrival		
	4.2	Ensure sufficient capacity both in transport and storage in the cloud, factoring in potential growth		
	4.3	Assess application compatibility		
	4.4	Ensure security of data in transit and at rest in the cloud		
	4.5	Plan for data transit to/from and storage at a COOP/DR site		
Governance	5.0	Identify need for new or changed governance		9
	5.1	Identify the current governance in place (the “As-Is”)		
	5.2	Identify governance needed to support the new cloud-based architecture (the “To-Be”)		
	5.3	Compare the two sets of processes to identify needed changes/updates, additions and deletions to establish a new governance baseline		
	5.4	Develop, document, and coordinate new or amended governance with the stakeholders (users and supporting staff) to ensure it meets the intended goals and does not cause any unintended consequences.		
	5.5	Eliminate governance and related processes no longer needed.		

Category	WBS Index	Action	Approach	Reference Section
	5.6	Notify personnel of changes and provide training as required.		
Facilities	6	Consider facility impacts caused by the new environment (impact to office spaces, ability to free up unneeded space, etc.)		10

Attachment 4. References

1. DESMF: DoD Enterprise Service Management Framework (DESMF), Edition III, 4 Mar 2016 (http://dodcio.defense.gov/Portals/0/Documents/DESMF%20EDITION%20III%20Signed%20June2016.pdf)

2. ITIL: The IT Service Management Forum, "An Introductory Overview of ITIL® 2011" (https://www.tsoshop.co.uk/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf)

3. NIST: Cloud Reference Architecture (NIST SP 500-292) (http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505)

4. P3M3: Introduction to P3M3, Version 3, July 2016 (https://publications.axelos.com/p3m3/Guide/Introduction.aspx)

5. WBS:
    a. INCOSE, "Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, 4th Edition," 2015. (http://www.incose.org/ProductsPublications/sehandbook)

    b. Project Management Institute, "A Guide to the Project Management Body of Knowledge, 6th Edition." (https://www.pmi.org/pmbok-guide-standards).

    c. The MITRE Corporation, "Systems Engineering Guide," 2014. (https://www.mitre.org/publications/systems-engineering-guide/about-the-seg)

6. Cloud Security: Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," 2017 (https://cloudsecurityalliance.org/download/securityguidance-v4/).

This page intentionally left blank.

Attachment 5. List of Acronyms

Acronym	Meaning
AoA	Analysis of Alternatives
CIO	Chief Information Officer
CIKR	Critical Infrastructure Key Resource
CMDB	Configuration Management Data Base
COOP	Continuity of Operations Plan
CSP	Cloud Service Provider
DESMF	Department of Defense Enterprise Service Management Framework
DR	Disaster Recovery
GSA	General Services Administration
HVAC	Heating, Ventilation, and Air Conditioning
IaaS	Infrastructure as a Service
ID/IQ	Indefinite Delivery/Indefinite Quantity
IT	Information Technology
ITIL	Information Technology Infrastructure Library
O&M	Operations and Maintenance
OLA	Operating Level Agreement
P3	Portfolio, Program, and Project
P3M3	Portfolio, Program, and Project Management Maturity Model
PaaS	Platform as a Service
PfM	Portfolio Management
PjM	Project Management
PM	Program Management
POA&M	Plan of Action and Milestones
PWS	Project Work Statement
QA	Quality Assurance
QoS	Quality of Service
RACI	Responsible, Accountable, Coordinated, Informed
SaaS	Software as a Service
SDN	Software Defined Network
SLA	Service Level Agreement
SOO	Statement of Objectives
SOW	Statement of Work
WBS	Work Breakdown Structure