EPA Hosting Readiness Assessment Process

Table of Contents

Introduction

Purpose of the Readiness Assessment

EPA's Office of Environmental Information (OEI) is working with Agency System Owners to assess the readiness of IT systems to ensure the advantages of cloud hosting opportunities are realized where applicable. This effort is consistent with the Federal Cloud Computing Strategy (February 8, 2011) and ongoing OEI initiatives to achieve IT cost and performance efficiencies. It is also consistent with the CIO's responsibilities under the Federal Information Technology Acquisition Reform Act (FITARA).

Given the variety of cloud hosting options and models for federal systems, System Owners benefit from consultative services in assessing those options. The decision to stand up a new application or migrate an existing application to the cloud requires decision makers have a deeper understanding of the application architecture, operational requirements, business requirements, and security requirements in order to make the most well-informed decisions. New applications being developed can and should be architected to take advantage of the capabilities within the cloud target while meeting business and security requirements. For existing applications, decisions must be made regarding return on investment for migrating to the cloud. Existing applications rarely transition seamlessly from a traditional hosting environment to a public cloud vendor environment, as they often require some level of modernization, adjustments to code, and/or refactoring to take advantage of public cloud-based features such as scaling to de-allocate underutilized resources. Additional costs associated with transition can offset potential savings and push return on investment (ROI) beyond an acceptable window. Without a detailed assessment, these costs are often not fully understood until after decisions to migrate have already been made.

For these reasons, OEI has developed a comprehensive hosting readiness assessment methodology that captures critical data for making informed decisions. This methodology incorporates a comprehensive alternative analysis and documentation of a business case that aligns with EPA's operational, business, and financial constraints. The hosting readiness assessment process can be used by individual program offices to support Capital Planning and Investment Control (CPIC) decision-making processes and may also be incorporated into Software Lifecycle Management processes that each office uses to review, approve, and manage system development.

Readiness Assessment Roles and Responsibilities

The readiness assessment will be performed jointly between System Owners and OEI resources. The assessment begins with an initial readiness assessment by the System Owner using a simple pre-assessment/screening checklist. This step documents the status of the system and the potential cloud services that may be appropriate for the system. System owners will also provide key information from existing repositories and architecture diagrams so that analysis can take place that answers the question, is this application a potential candidate for the cloud?

After the System Owner completes the pre-assessment/screening checklist, NCC Project Managers and Cloud Analyst SMEs will collaborate with the System Owner to assess the readiness of the system for cloud hosting against multiple criteria: business/technical architecture readiness, financial and risk factors, and organizational readiness for managing the system in the cloud. This second step delivers a more thorough assessment, including options analysis, to help System Owners determine the type of hosting solution that is best suited for that system: an internal private cloud hosting service offering through the National Computing Center (NCC), third-party hosting by an outside vendor (including the Agency's cloud.gov solution) or a hybrid cloud deployment using some combination of the two.

Reporting the Hosting Readiness Assessment Results

The assessment results will be summarized in a short readiness assessment memorandum to the CIO and be utilized as part of OEI's FITARA review. This memorandum will outline the factors for and against cloud hosting of the system and provide a recommendation for the future state of the system's hosting solution.

Considerations for Evaluating System Readiness

When evaluating the readiness of a system for cloud hosting, the Agency has multiple options for consideration, as shown in Table 1.

Table 1. Characteristics of NCC-Brokered Hosting Options

Hosting Option	Traditional Characteristics of a System Hosted
Internal Private Cloud Services	A cloud environment built and maintained by NCC for EPA users with controlled access through identity management. NCC acts as a service broker of the internal private cloud services.
Third-Party Cloud Services	Cloud hosting offered by OEI-approved third-party (non-EPA) vendors in which the System Owner provisions hosting services needed from the vendor .
Hybrid Cloud Services	Cloud hosting that utilizes some combination of Internal Private and Third-Party clouds to support hosted applications or systems.

When evaluating these models, System Owners must bear in mind the various services required for operation of the system within the environment, including responsibilities across potentially multiple service providers. Table 2 provides insight into various hosting models.

Table 2. Ownership and Responsibility under Different "As-a-Service" Models

"As-a-Service" Hosting Model	Typical Ownership and Responsibility	Notes
Infrastructure as a Service (IaaS)	• Server, storage and network are the responsibility of the IaaS provider • Data and applications are maintained by the System Owner • IaaS provider charges for provision of infrastructure, typically on a utilization basis	• Requires clearly defined responsibilities between/among the infrastructure provider and the System Owner/application service providers related to key service components including but not limited to network, security, software upgrades, etc.
Platform as a Service (PaaS)	• Server, storage, and network are the responsibility of the PaaS provider • PaaS provider also provides operating system and middleware necessary for a System Owner to run the application • PaaS provider charges for provision of infrastructure, OS, and middleware, typically on a utilization basis	• Requires clearly defined responsibilities between/among the for PaaS service provider and the System Owner/application service providers related to key service components including but not limited to: software upgrades, network upgrades, security, etc.
Software as a Service (SaaS)	• Server, storage, network, operating system, middleware, and software delivered by the SaaS provider • SaaS provider frequently prices based upon a per use basis	• SaaS provider delivers a full service, augmented by the System Owner in order to meet discrete business needs (e.g., specific agency security requirements)

Often, additional investment is needed to support an application's optimum operation within the cloud. Decisions to be made by the System Owner may include the system redesign decisions shown in Table 3, based upon a detailed cost-benefit analysis.

Table 3. Example System Redesign Considerations

System Redesign Decision	Typical Activities and Factors in Hosting Decision
Re-host (move) a system architecturally as is	Redeploy an application to a cloud-based platform without modifying the application's code
Refactor a system	Make application code or configuration changes to connect the application to an infrastructure or platform as a service provider's infrastructure
Revise the system	Modify or extend the application's code base to support legacy modernization requirements and then use the re-host or refactor options to deploy it to the cloud
Rebuild the system	Redevelop the application on a provider's platform as a service offering
Replace the system	Eliminate the former application and replace it in an external platform

Source: Gartner, Devise an Effective Cloud Computing Strategy by Answering Five Key Questions, November 2015

Conducting the Readiness Assessment

Step 1 – Pre-Assessment: Qualifying the Application's Cloud Readiness

The pre-assessment process is designed to quickly collect high-level business, operational, and technical data about the application and to identify common areas that may indicate risk and cost factors. This step begins with a self-service questionnaire, to be completed by the System Owner (within the input of relevant stakeholders). Questions are specifically tailored to business, operational, and technical stakeholder language to ensure those asked to provide the information can provide the answers quickly.

The pre-assessment provides a means to:

- Gather technical and non-technical information about the application
- Establish a baseline understanding of the current environment and service level objectives required to support the customer needs
- Identify goals and drivers for moving the application to a Cloud environment
- Evaluate the requirements against a set of known risk factors

To further reduce the time to complete, the Pre-Assessment uses multiple choice questions specifically designed to expose critical information not obtainable through simply a review of technical data. Using the multiple choice Pre-Assessment, application stakeholders select the best fit answer from the options provided, understanding that the purpose is to only pre-assess the potential of the application for operation within a cloud target. As part of the Pre-Assessment process, we further request certain supporting documentation that can be used by the NCC Project Management staff in evaluating whether the application is a good candidate for migration to the cloud.

Output of Step 1 Pre-Assessment: As an output of the Pre-assessment step, System Owners receive a Pre-Assessment Report. Those systems deemed to be potential cloud migration candidates will move on to Step 2 analysis. For those systems determined to not be good cloud migration candidates as currently architected, OEI provides a summary of findings to the System Owner with justification and, where applicable, suggestions for remediation to support future cloud migration.

Step 2 – Detailed Cloud Readiness Analysis: Evaluation and Recommendations

Assuming that no information within the pre-assessment precludes operation of the application within a cloud environment, OEI and the System Owner will collaborate in further analysis and evaluation of:

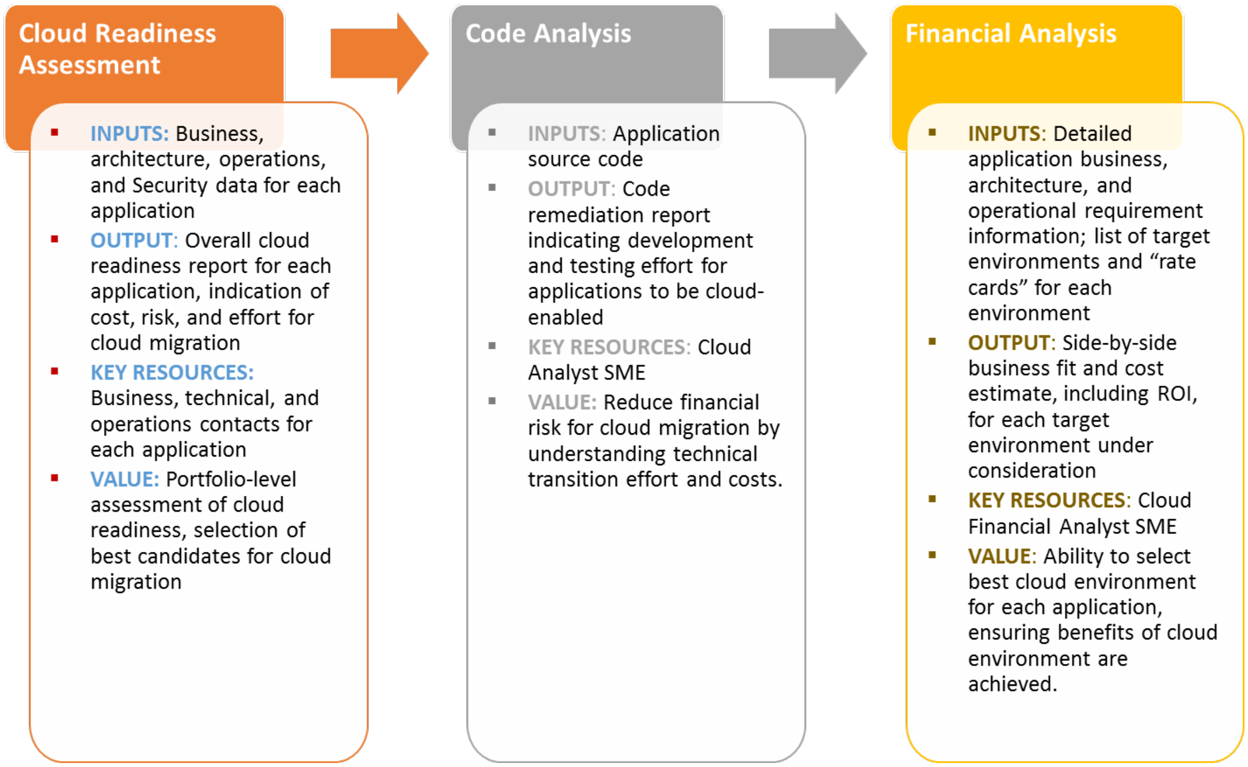
1. Overall cloud readiness fit in the areas of risk, cost and level of effort
2. Areas for system remediation that that may be necessary in order to host an existing application in the cloud
3. Comprehensive comparison of multiple potential cloud targets, encompassing transition costs, estimated remediation costs, and annual operating costs for each of the alternatives evaluated

The Cloud Readiness Analysis delves deeper into the system's architecture and technical foundation and requirements, business objectives, cost elements, risk, as well as governance and organizational considerations, in order to collaboratively chart a course for the most cost-effective location for operation of the system.

The overall process for the detailed Cloud Readiness Analysis is broken up into three phases:

1. Business, Technical and Operations reviews utilizing a combination of tools and questionnaires, answered through a series of interviews.
2. Software analysis of existing applications to determine technical fit and readiness. This phase is not conducted for "planned" or "new" applications.
3. Detailed financial and business analysis providing for comparisons between multiple hosting options.

Figure 1 provides an overview of these three phases including a snapshot of the key inputs to the phase, outputs delivered, and key resources required to accomplish phase objectives.



Cloud Readiness Assessment

- **INPUTS:** Business, architecture, operations, and Security data for each application
- **OUTPUT**: Overall cloud readiness report for each application, indication of cost, risk, and effort for cloud migration
- **KEY RESOURCES:** Business, technical, and operations contacts for each application
- **VALUE:** Portfolio-level assessment of cloud readiness, selection of best candidates for cloud migration

Code Analysis

- INPUTS: Application source code
- OUTPUT: Code remediation report indicating development and testing effort for applications to be cloud-enabled
- KEY RESOURCES: Cloud Analyst SME
- VALUE: Reduce financial risk for cloud migration by understanding technical transition effort and costs.

Financial Analysis

- **INPUTS**: Detailed application business, architecture, and operational requirement information; list of target environments and “rate cards” for each environment
- **OUTPUT**: Side-by-side business fit and cost estimate, including ROI, for each target environment under consideration
- **KEY RESOURCES**: Cloud Financial Analyst SME
- **VALUE**: Ability to select best cloud environment for each application, ensuring benefits of cloud environment are achieved.

Figure 1. Cloud Readiness Analysis Phases

While this process is described in phases, note that these phases need not occur sequentially. However, outputs from the cloud readiness assessment phase and code analysis phase (an optional phase targeted for Java and .NET applications to assess potential refactoring needs) directly feed and are key inputs to the financial analysis phase.

Leveraging industry-unique tools and supporting processes, NCC Project Managers and Cloud Analyst Subject Matter Experts support System Owners in conducting the cloud readiness analysis, analyzing changes that may be required to the system in order to optimize operation within the cloud, and evaluating the various cloud hosting options available in the market for business fit, cost, risk, and level of effort for an assessment of return on investment. Throughout the process, NCC Project Managers, Cloud Analyst SMEs, and System Owners work together to evaluate various architectural options, enabling a more accurate “apples to apples” evaluation of how a system may operate in a given environment. We collaborate in analysis and evaluation of business, technical, and security needs (e.g., are high availability/disaster recovery capabilities to meet service level objectives or incorporation of additional non-production environments) and how those considerations may impact the overall to-be configurations and costs in each potential cloud target.

Through this detailed assessment, NCC Project Managers, Cloud Analyst SMEs, and System Owners collect information to address questions associated with the overall solution architecture and technical requirements, business needs, financial impacts and risk considerations, as well as the governance and organizational model that may be needed to support operation within a cloud paradigm. The following are examples of essential questions the assessment seeks to answer.

Architecture/Technical

1. Is the system's current or planned architecture amenable to a cloud hosting architecture? What changes would need to occur to the application for cloud hosting?
2. What are the costs and opportunities for refactoring the architecture to be optimized for the cloud?
3. What operating system, databases, and software applications are in use and are these amenable to migration to the cloud?
4. What are the CPU, bandwidth, memory, network, and storage requirements and can these be provided in the cloud?
5. What are system dependencies and system interfaces that are necessary? Can these be met in the cloud?
6. Are there any dependencies on proprietary devices, applications, licenses, hardware, or software that cannot be met in the cloud?
7. Can disaster recovery, continuity of operations, and monitoring be met through a cloud hosting solution?
8. What are the service levels required to meet business needs, and can required service level agreements be met through cloud hosting?
9. Can security, access, data protection, and data controls be met through a cloud hosting solution? Can all regulatory requirements for the system be met through cloud hosting?

Business

1. Is the business model amenable to a cloud hosting environment?
2. Is there an impact on any user communities as a result of move to the cloud (e.g., lack of access for any user groups)?

Finance and Risk

1. What is the best hosting environment for the application based on business requirements and financial needs?
2. What are the estimated lifecycle operations and maintenance costs on an annualized and projected out year basis?
3. What are the potential areas of risk as well as the costs associated with managing or mitigating the risks?
4. What is the level of effort required to modernize (e.g., refactor, revise, rebuild) and level of effort costs for modernization and migration?

Governance and Organizational Considerations

1. Are there agreements and practices in place among all parties for the governance of the system in the selected hosting environment? If not, can they be established?
2. Are there clear organizational roles and responsibilities established that correspond the governance requirements of the selected hosting location? If not, can they be established?
3. Does the organization have the IT skills in place (or easily accessible) to maintain the new hosting environment?

Output of Step 2 Cloud Readiness Analysis: The Cloud Readiness Analysis results in a documented report that details the analysis and evaluation conducted. This report is designed to support informed decision-making regarding to-be hosting architectures based upon the detailed assessment findings as well as a comparison of cloud service provider offerings (i.e., potential cloud targets). The report includes a general “Readiness Index” score, made up of individual scores in the areas of Risk, Cost, and Level of Effort. The report also includes financial options analysis findings that incorporate evaluation of comparative services offerings from multiple potential Cloud Service Providers (and potentially different cloud service models – for example, IaaS or PaaS). Where decisions must be made regarding investments such as refactoring or revising a system, the report may include recommendations or further points of investigation by the System Owner. The objective of the report is not to dictate a cloud migration path and target or modernization plan but, rather, to empower System Owners to make informed IT investment decisions based upon a thorough analysis and evaluation of risk, cost, and level of effort.

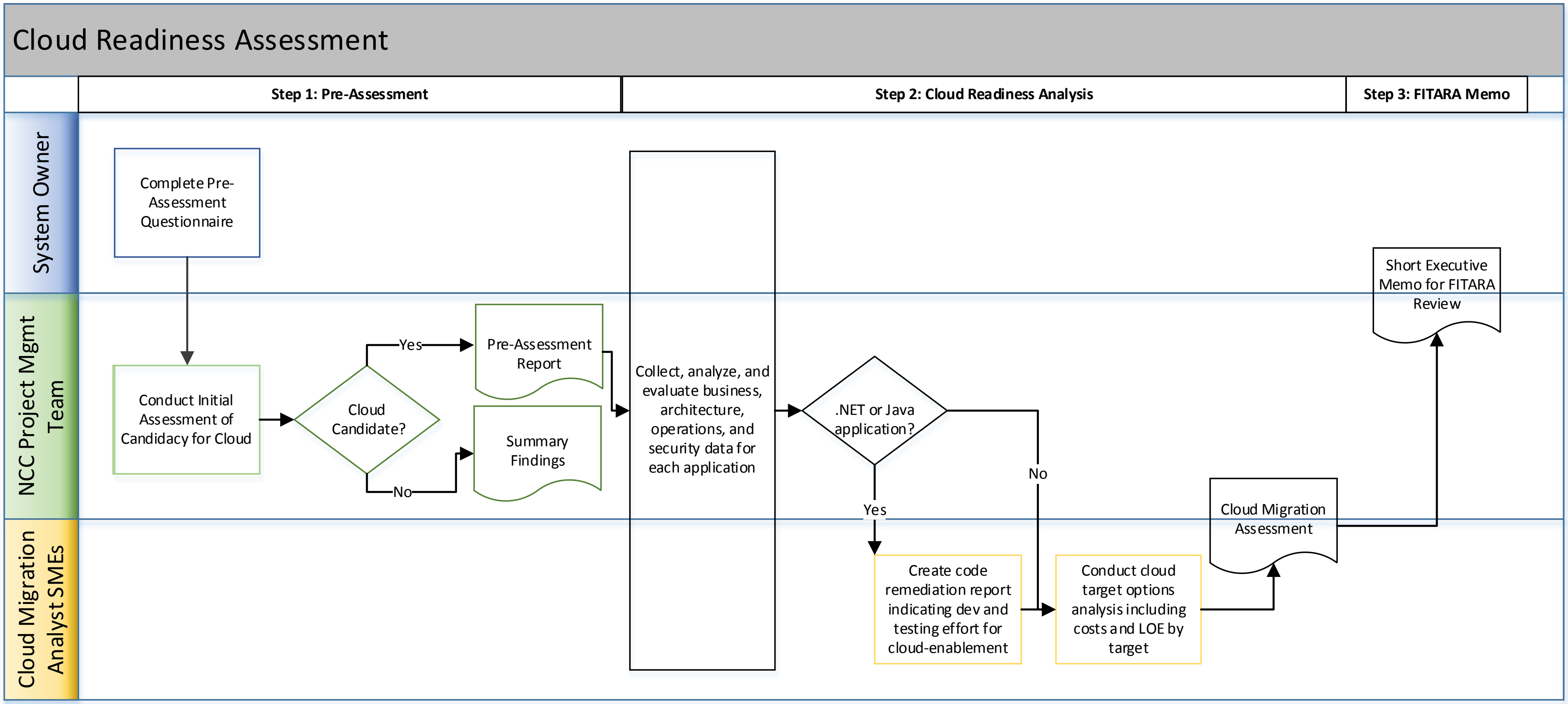
Step 3 –Executive Memorandum for FITARA Review

The sharing of information with the EPA CIO regarding the system investments is an important step within the EPA’s FITARA review process. To support this review, OEI includes a collaboration with System Owners as Step 3, resulting in a memo describing the outcome of the assessment.

Output of Step 3 Executive Memo: The memo provides high-level outcomes of the assessment, recommendations for future hosting decision, and cost data to support the FITARA review. To simplify this step, OEI has created a standardized format for the memo that includes the following:

- Brief Description of the System (1-2 paragraphs)
- Current Hosting Location and Hosting Costs (for existing systems)
- Summary Results of Pre-Assessment and Cloud Migration Assessment
    - Architecture/Technical Summary
    - Business Summary
    - Finance and Risk Summary
    - Governance and Organizational Considerations
- Recommendation for Future Hosting Decision

Hosting Readiness Assessment Process Overview


Cloud Readiness Assessment
Step 1: Pre-Assessment
Step 2: Cloud Readiness Analysis
Step 3: FITARA Memo
System Owner
NCC Project Mgmt Team
Cloud Migration Analyst SMEs
Complete Pre-Assessment Questionnaire
Conduct Initial Assessment of Candidacy for Cloud
Cloud Candidate?
Yes
No
Pre-Assessment Report
Summary Findings
Collect, analyze, and evaluate business, architecture, operations, and security data for each application
.NET or Java application?
Yes
No
Create code remediation report indicating dev and testing effort for cloud-enablement
Conduct cloud target options analysis including costs and LOE by target
Cloud Migration Assessment
Short Executive Memo for FITARA Review