Application Lifecycle Framework

February 2021

Introduction

This document provides high-level guidance for moving applications from on-premise locations to cloud environments, not for new cloud-native deployments. This framework outlines the process necessary to move an application to an existing CSP, and as a result assumes that the agency has existing cloud design documents, architecture, and operations guides for their enterprise cloud environments. This document is focused on providing information to agencies interested in pursuing Lift and Shift migrations using an Infrastructure-as-a-Service (IaaS) CSP, and not for Platform-as-a-Service (PaaS) and Software-as-a-Service CSPs. The steps and templates included in this framework seek to provide a notional list of potential tasks for your agency's application migration but should not be considered a mandatory checklist of requirements for every agency or for every application.

Table of Contents

1. Application Submission

❐ Submission Request

This should express your business need. Articulate the functional and capability requirements along with the desired outcomes, not a specific technology solution.

❐ Business Data

This information can be included in the Submission Request, including

- Resources required to manage application
- The purpose of the application and/or mission delivery value
- Existing application Service Level Agreements (SLAs) to customers
- Performance history (e.g., uptime/availability requirements), application health

Use your Submission Request findings as an input to this task.

❐ Project or Product Manager Assigned

Formally assign a project or product manager for application migration efforts, ideally with an official sign-off from the Cloud Operations team.

❐ Application Stakeholders

Identify all relevant stakeholders. Please refer to the Cloud Strategy Guide’s Stakeholder Analysis section for assistance.

Key Concept

Begin submitting requirements and creating a project plan. The documents and steps at this stage help you identify stakeholder, process, and project management considerations for your agency’s migration through data gathering, migration process planning, and initial stakeholder discussions.

Resources and Templates

Application Migration Project Template

Application Business Plan

❐ Establish Document Library

Start a document repository for the application and make sure all stakeholders have access.

❐ Create Project Plan

Once the project manager is assigned, develop a project plan according to your agency’s methodology.

❐ Initiate Governance Planning

Discuss governance requirements with application business owners and create a plan for the management and governance of security and other operational concerns for the shared responsibility model of using cloud service providers (CSPs).

2. Current-State Analysis

❐ Evaluate Discovery and Assessment Tools

Determine the Tool to use for Discovery and Assessment of your on-premises inventory, including your IT workforce and governance, security, and network. There is a marketplace with numerous available options, a good starting point for your agency would be looking at existing FEDRAMP-approved processes and services.

❐ Discovery and Assessment

Discover and document existing technical state that includes:

- Application/Server locations;
- Software builds, versions, components;
- Existing architecture and design documents; and
- Existing IT governance, IT workforce, and change management processes.

❐ Determine Cloud Service Provider

Determine best CSP based on discovery, assessment, and dependencies.

❐ Initial Security Assessment

Review current ATO and security requirements with the system owner and Information System Security Officer (ISSO). Compare existing security profile and requirements with future state cloud ATO requirements.

Key Concept

The goal of this stage in the framework is to evaluate people (functions, roles, capabilities), processes (frameworks, reviews, procedures/guidelines), and technology (databases, solutions, tools) across the agency. The current state analysis should help you understand the interdependencies and strengths of your current environment.

Resources and Templates

Server Collection Worksheet

CSP Estimate Template

CSP Capacity Collection Template

Application POCs

❐ Contract and License Information

Acquire existing contract and licensing information that pertains to hardware, software, and labor. Inventory Current Software Licensing and Maintenance Agreements and ensure you understand the details regarding your CSP licenses. Some Cloud Service Providers (CSPs) write their agreements where they require a license per vCPU. List Software licensing model (e.g., seats, servers, clients) for all applications, including cost and length of term. Document and review your open-source software, adhering to OMB M-16-21 requirements. Determine which of these licenses can be used in the Cloud once Cloud Service Provider (CSP) determination is made.

❐ Determine Cloud Readiness

Perform the cloud suitability assessment based on discovered inventory and applications, considering security, architectural and functional criteria.

❐ Cloud Cost Estimate

Create estimated hosting and management cost for applications based on business data using your CSP’s cost estimator or agency specific methodology.

❐ Application Info & Dependencies

Determine Application Configuration Data:

- Code, APIs, COTS, Ports, Databases, Security and Dependencies to other applications.
- Application Dependency Map
- Technology Refresh Cycles
- Hardware at End of Life / Support
- License / Software Maintenance Renewal Dates

❐ Firewall, Ports, and Protocols Determination

Provide information security requirements criteria to the cloud readiness assessment process. Determine ports, protocols, and firewall requirements.

❒ Workforce Assessment

Ensure your existing workforce has the skills, knowledge, and abilities needed to successfully adopt cloud platforms, move applications to the cloud, or purchase commercial cloud services. Further details and guidance are available in the “Workforce” section of the Cloud Strategy Guide.

❒ Update Document Library

Update document library based on output from completed activities.

3. Provision Target State

❐ Migration Methodology

Determine which migration platform is best suited for your application or workload based on your discovery and assessment results. Consult with your CSP engineering representative to identify appropriate native solutions or consider third-party solutions where applicable.

❐ Create Application Configuration Document

Outline the application configuration and supporting services within the hosting environment in the cloud. Ensure all relevant configuration information is documented in the design document. Identify CSP VNETs, VPCs, CIDR, and subnets. Reference your agency's existing cloud design document and operations guide.

❐ Cloud Application Architecture Diagram

Take a structured approach to designing your cloud application hosting environments, using architecture designs that cater to the offerings of your CSP and design principles. Consider setting standards or create a reference architecture for the enterprise. Reference your agency's existing cloud architecture diagram.

❐ Cloud Capacity and Assessment

Determine your cloud capacity requirements, such as total CPUs, memory, instances or VMs, databases, load balancers, subnets, CIDR block, or IPs & Ports. Document this information in the application design document.

Key Concept

Determine your migration methodology and complete documentation and other requirements. This ensures success for your configuration, application architecture, capacity, and security considerations (i.e., firewalls, ports, and user access requirements). Completing these tasks allows for necessary technical documentation to be recorded and services in the target cloud environment to be provisioned. This step also includes beginning your cloud assessment and ATO process.

Resources and Templates

ATO Checklist

CSP Account and Resource Request Form

Firewall Request Template

❒ Firewall and Ports Submission

Use existing processes to ensure proposed changes are viable and will not adversely impact the operation of the existing system or subsystem. Implement a review board to review all requests. See the “Governance” section of the Cloud Strategy Guide for further details.

❒ Establish Security Groups and Requirements

Implement required security groups and access control lists (ACLs) in your cloud environment. Record security groups in the application configuration document. Implement security requirements based on FIPS 199 categorization and FISMA requirements.

❒ Cloud Resource Request

Identify and submit a cloud service resource request. Conclusions on cloud resource requirements should be determined in Step Two, Current State, and the Discovery/Assessment Reports.

❒ Start Authority to Operate (ATO) Process

Work with ISSO to begin the process to acquire a new ATO for the system when migrated to the cloud.

❒ User Access Requirements

Identify and document users that need to use the application as well as application administrators that need access to the cloud environment to perform engineering or maintenance tasks.

❒ Update Document Library

Update document library based on output from completed activities.

4. Provision & Acceptance

❐ Cloud Environments Provisioned and Accessible

Work with stakeholders to review provisioning documentation, gain formal agreement, and provision the target state cloud environment. Stakeholders may include the application team, cloud operations/engineering, and the corresponding CSP account lead or engineer.

Example documentation can include:

- Resource Request Form
- Cloud Capacity Form
- Cloud Application Architecture Diagram
- Cloud Cost Estimates
- Gain formal agreement, and provision the target state cloud environment.

❐ User Accounts Created

Account management team creates cloud user accounts based on the user list documented in Step 3 “User Access Requirements.”

❐ Portal and Cloud Access/Jump Box

Privileged users identified and accepted in the CSP resource request form will be granted portal and jump box access to the target environment.

Key Concept

This stage should be used to finalize the preparation of the cloud environment by first ensuring resources in the cloud environment are accessible by your agency, then preparing for on-boarding with your CSP.

❐ CSP On-Boarding

Once the application owner accepts provisioning, the agency cloud operations and CSP Account representatives conduct an onboarding meeting with the application team. Use this meeting to go over the technical details of their environment, including how the application team accesses their environment.

❐ Assign Cloud Migration Project Manager

Formally assign a project manager to manage the technical migration of the application to the CSP.

❐ Update Document Library

Update document library based on output from completed activities in this process.

5. Migration Planning

❒ Confirm Firewall Ports/Dependencies

Confirm the firewall rules submitted to the Review Board are approved and open for the migration/cutover window. Also make sure that all security groups/ACLs ports and rules are in place.

❒ Migration Plan

Cloud project manager and application team develop migration schedule according to agency methodology. Cloud migration does not have to happen all at once. You can migrate services in phases or waves grouped by service or user. Consider the following tasks for your migration plan:

- Complete replication testing
- Finalize Migration Checklist
- Set a cutover date
- Communicate plan to all stakeholders
- Ensure your systems are ready to transition to the target cloud

❒ Finalize CSP VNETs, VPCs, Subnets

Finalize all relevant configuration items and update your application configuration document.

❒ Finalize Cloud Migration and Hosting Costs

Update and finalize hosting and migration costs based on any new or updated information identified in the discovery process.

Key Concept

These planning steps provide a last review of necessary tasks before your application is migrated to your agency’s cloud environment. The goal is to finalize contingency plans, a migration schedule, and licensing, while preparing a strategy post-migration to decommission your application from on-prem.

Resources and Templates

CSP Estimate Template

App Migration Questionnaire

Migration Checklist

Application Sprints

Decommissioning Checklist

❒ Rollback Plan

Include a phased, cutover approach in your project plan to allow for rollback points if things are not going according to plan and reduce migration risk. Ensure your rollback plan is documented and approved by relevant stakeholders.

❒ Apply Tagging Taxonomy

Use your existing cloud-tagging strategy for target-state services. See the “Governance” section of the Cloud Strategy Guide for more details.

❒ Prepare Workforce

Ensure your workforce is trained on operating the application in the new cloud environment.

❒ Disaster Recovery

Develop a disaster recovery plan outlining how application can be restored to its original state in case of system faults, disasters, and other catastrophic events.

❒ Backup Plan

Develop a “cloud backup plan” that is adapted to your agency’s backup storage needs. Utilize the CSP centralized management interface to make it easy to define backup policies and protect a wide range of enterprise workloads.

❒ Finalize Contracts and Licensing

Acquire licensing required to migrate and operate applications in the cloud environment.

❒ Create Decommissioning Checklist

Application retirement, also called application decommissioning, is the practice of shutting down on premise business applications that have successfully migrated to the cloud. Create a checklist to decommission the existing on-premises application once migrated to the cloud.

❒ Document Orchestration Templates

The cloud orchestration approach provides several benefits and can be accomplished using templates. Create management templates for routine application tasks.

❐ Start On-Prem Replication

Approaches vary depending on the migration methodology but involves cloning on-prem environments to maintain the current state. The replication process is the prelude to the final migration, which is the cutover.

❐ Update Document Library

Update document library based on output from completed activities.

6. Migration Day

❐ Communicate Migration Agenda

Communicate a detailed migration agenda to stakeholders, an example of which is included in the Resources and Templates section of this step. It is recommended to communicate this agenda via email as part of preparation of migration day. Be sure to communicate both the cutover window and the actions that transpire within that window (with time frames).

❐ Execute Migration Plan and Cutover

Start your migration checklist. This cutover action varies depending on the migration platform and methodology you are using. Some cutover actions include:

- Update your enterprise DNS records to reflect the applications new IP scheme.
- Test and ensure all required firewall ports are open to support the application migration and production usage.

❐ VM Tasks

This varies by VM type and the type of services the Agency runs on their VMs. Example tasks include:

- Update the hostname and IPs;
- Configure databases; and
- Run automated scripts to install specific services.

Key Concept

This stage is about all the steps you will complete on the day of the migration. In addition to the migration itself, it involves preparatory communication work and includes testing to ensure success of your application in the cloud environment before the migration is finally accepted.

Resources and Templates

CSP Capacity Collection Template

ATO Checklist

Migration Checklist Example

❐ App Testing, Database Testing, User Testing

Conduct structured testing of the application in the new hosting environment. Typical testing can include the following testing actions:

- Check that hostname and IP resolve properly;
- Validate user access;
- Check SSL certs;
- Check connectivity of application and application functionality;
- Run vulnerability scan; and
- Run validation tests

❐ Migration Acceptance

Complete all migration actions and get formal approval from the application owner to confirm migration has successfully completed.

❐ Update Document Library

Update document library based on output from completed activities.

7. Operations

❐ ATO Completed

The new application ATO has been completed and signed by the Designated Approval Authority.

❐ Application Monitoring

Use a series of cloud-native tools to monitor your applications. For more details, refer to the “Target-State Environment” section of the Cloud Strategy Guide.

❐ Implement Cost Portal

CSP cost portals let you visualize, understand, and manage your CSP costs and usage over time. Create a custom portal or use one provided by your CSP to identify trends, pinpoint cost drivers, and detect anomalies.

❐ Implement Security Advisor

CSP security advisor gives you a comprehensive view of your security alerts and security posture across your CSP accounts. Within your CSP security advisor, you have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple CSP services.

Key Concept

The aim of this step is to establish standard operating procedure for your applications in the cloud, keeping in line with your governance strategy. The components in this section should help ensure your agency is secure and operationally and financially successful post-migration.

Resources and Templates

CSP Capacity Collection Template

ATO Checklist

Migration Checklist Example

❒ Update Operations Guide

The operations team needs to update the operations after migration. A typical operations guide outlines all required actions and processes to maintain an application in a hosted environment. It ensures that cloud operations are efficient in using required resources as well as meeting quality of service requirements, compliance requirements and especially customer satisfaction.

❒ Documentation Finalized

Finalize all documentation used for the migration (application configuration document, architecture document, project plans, etc.). Prepare the documents for storage and long-term reference within the document library.

❒ Update Document Library

Update document library based on output from completed activities.

8. Decommission On-Premises Systems

❒ Run Decommissioning Checklist

After your migration is complete and formal acceptance is achieved, follow a structured process to decommission on-premise applications and services (i.e., shutting down on-premise VMs and systems). Reference the Decommissioning Checklist as an example.

❒ Contract Terminated

If you need to terminate any contract agreements post-migration, be sure to do so at this time.

Key Concept

Ensure that you have properly decommission existing systems and services once your application is functioning as expected in a cloud environment.

Resources and Templates

Decommissioning Checklist