CMS Target Life Cycle

Overview

June 6, 2022

Table of Contents

I. Introduction

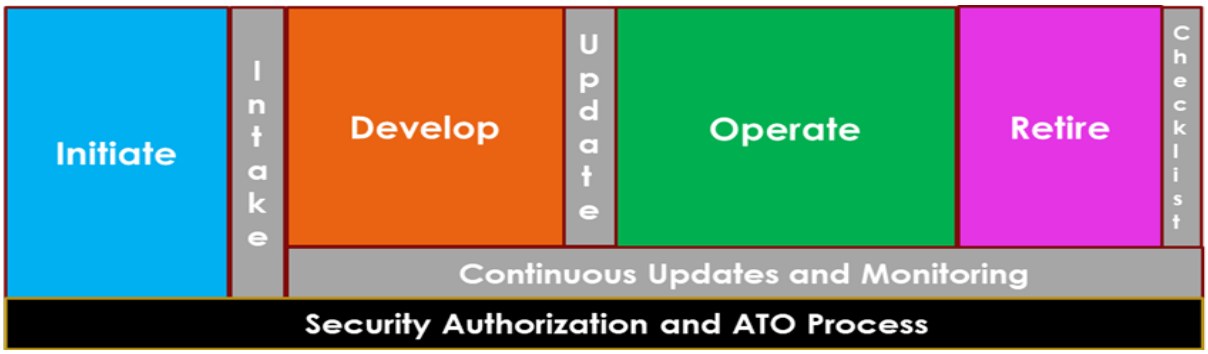
The Centers for Medicare & Medicaid Services (CMS) commits to empowering business flexibility in IT system development, making sound investment decisions, and complying with Federal IT laws and regulations. The TLC replaces the creation of prescribed artifacts with business flexibility, and replaces point-in-time gate reviews with consultations, continuous evaluation, and situational reviews. Figure 1 illustrates the four phases of the TLC.

Key Concept #1: Business Owner Responsibility – The Business Owner is responsible for ensuring that the System Maintainer has adopted and is complying with a suitable Systems Development Lifecycle Methodology for documenting requirements, development, and testing of the solution, as well as managing risk. This will allow flexibility in selecting the documentation method and repositories best suited to the chosen methodology rather than prescribing specific processes. Governance will not be reviewing those artifacts on an ongoing basis, but they must be available to satisfy internal and external audits.

Key Concept #2: Situational Governance – During the development and maintenance phases, CMS will apply situational governance. The Business Owner should document any significant changes to the project scope in the CMS System Census and in CFACTS, for governance review.

This approach will allow for the least possible governance overhead while still ensuring that CMS systems are securely developed and properly supported.

Figure 1. CMS Target Life Cycle



II. CMS Target Life Cycle Phase Summary

A. Initiate Phase

This process will rely heavily on the guidance and assistance of the EA team, Navigator, Subject Matter Experts (SMEs), Technical Review Board (TRB), and the Governance Review Team (GRT) to help the Business Owner to develop, document, and evaluate potential options for development. The Business Owner should consult with the TRB representatives from ICPG in the Initiate phase to begin the Security Assessment and Authorization process. The Project Team must consult representatives from Security, Privacy and Accessibility in the Initiate phase, and the Security Assessment and Authorization process begins.

B. Develop Phase

The purpose of the Develop Phase is to create the detailed user stories or requirements, design and develop the solution, deploy it to a non-production environment, and test it for compliance with the requirements and CMS standards so that it is production ready. The Business Owner must ensure all requirements, user stories, design, development and testing comply with the CMS Technical Reference Architecture (TRA), Acceptable Risk Safeguards and, privacy and accessibility standards (sections 504/508 of the disability act).

The Business Owner and Developer work collaboratively to determine the system development methodology. The TLC requires only a minimal set of artifacts, expecting components to follow best practices of their chosen Systems Development Life Cycle Methodology and Program Management methodology.

C. Operate Phase

The purpose of the Operate Phase is to maintain steady Production operations and to perform routine maintenance in accordance with sound security practices. The Business Owner and Developer complete any COTS upgrades, system software patches, hardware upgrades, and modifications to interfaces with other systems during this Phase.

D. Retire Phase

The purpose of the Retire Phase is to ensure compliance with Federal guidelines when retiring a government IT system. There are many aspects to consider such as records retention, information security, and investment close out procedures.

E. Available Resources

The project team has access to additional resources if situational governance is triggered. The CMS governance bodies are available for consultations on the need or expectations for guidance or reviews.

F. Capital Planning Investment Control (CPIC) and Security Assessment and Authorization

The TLC requires a fully vetted CMS Authority to Operate (ATO). Following all CMS ATO processes and procedures is necessary, as specified in the CMS Acceptable Risk Safeguards (ARS) and Risk Management Handbook. Program and Project managers must adhere to OMB requirements as well as CMS or HHS policies regarding IT investment management in accordance with CPIC Policy.

III. Initiate Phase

Initiate.	Intake	Key Objectives 1. Clarify business needs 2. Evaluate solution alternatives Exit Criteria 1. The Business Case and Analysis of Alternatives have been documented 2. An approved solution has been selected by the Business Owner 3. A Life Cycle ID (LCID) number has been issued

A. Overview

All new business needs and material changes to existing systems must go through the Initiate phase. Business owners must identify and justify their business needs and consider alternative solutions, in order to align to the CMS Business Reference Model and TRA and to comply with Federal laws and regulations.

During the Initiate Phase the Business Owner (and Navigator if assigned), will collaborate with the TRB and SMEs knowledgeable about CMS infrastructure, Technical Reference Architecture (TRA), and existing assets in order to define and document the general business need or enhancement, and explore and document solution options. The Business Owner should consider leveraging existing CMS/HHS Cloud Computing vehicles, i.e.: Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and Infrastructure-as-a-Service (IaaS) solutions. The project manager needs to assign an Information System Security Officer (ISSO), and begin collaboration with their Cyber Risk Advisor (CRA), and Privacy Advisor (PA) at this stage, to make an initial assessment of security risks and privacy considerations.

Collaboration with the SMEs and EA to develop and document the business need, recommended alternatives, and recommended budget is an iterative process. There is no specific order and often the business needs become clearer and gain detail after multiple rounds of discussion and questions.

The Business Owner must provide a fully developed business case and alternatives analysis prior to the Governance Review Board (GRB) meeting.

The GRB, consisting of the CMS Chief Information Officer (CIO), Chief Financial Officer (CFO), Head of Contracting Authority (HCA), Chief Technical Officer (CTO), Budget Development Group (BDG) members, and others will evaluate the potential solutions to ensure that they are making informed investment decisions to address the business need. The GRB may authorize one or more potential solutions for the Business Owner.

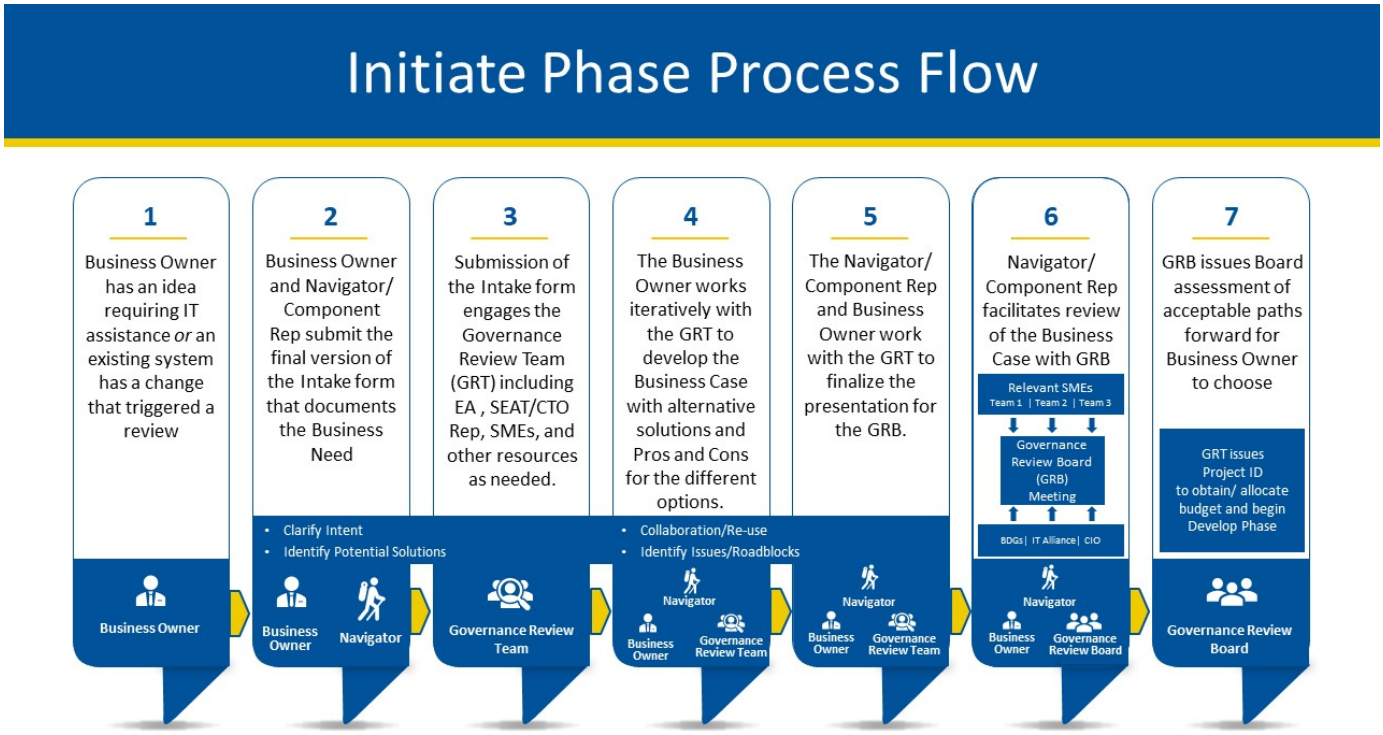
Upon selection of a solution authorized by the GRB, the Business Owner will engage the relevant components to arrange any necessary funding and contract actions before proceeding to the next phase, Develop.

The TLC requires the cooperation of all components in order to be successful and mitigate previous audit findings against CMS. The Initiate Phase is the key part of this new process, and it

will enable Governance to reduce oversight in later phases. The failure of multiple programs across the agency to comply with these new processes may require Governance to install more rigorous requirements as a remediation for Agency audit findings, such as additional documentation submission requirements in the TLC, stored and retained centrally.

B. Initiate Phase Detailed Flow

Figure 2: Initiate Phase Process Flow Diagram (Each column number corresponds to the step description below)



1. The Business Owner determines that there is a need for new or enhanced IT functionality. It could be a new system or changes to an existing system.
    a) System changes that may trigger a review generally include, but are not limited to, items such as:
        1) Data Center Migrations
        2) Software platform changes
        3) New system integrations/interconnections
        4) Changes in Major Function Alignments or the Data Categories a system supports

2. The Business Owner submits an Intake form in EASI. They may engage a Navigator to help them complete the form, or they may complete as much information as they have and submit the Intake form themselves.

b) Business components which do not have a Navigator may request that a Navigator from the Office of Information Technology (OIT) assist their project.

c) If a Navigator is not necessary, the component can fulfill the duties of the Navigator, including submission of the intake form and all steps up to and including presentation to the GRB meeting (step 6, below) including collaborative meetings with EA and TRB and the development of a Business Case including documentation of alternative solutions for consideration by the GRB.

Many IT acquisitions will not require a governance review. The Governance Review Adminstration Team reviews the Intake form that the Business Owner submits and later steps will often be bypassed, and an LCID will be issued for them immediately. They include acquisitions such as:

1) Recompete of an existing O&M Contract with no addition to scope
2) Cost increases for infrastructure or SaaS due to increased usage.
3) Bridge contract extensions due to contested contract awards
4) Renewal of an IAA

The LCID must be entered in the AP in the appropriate spot before sending the AP to Governance for signature.

3. The GRT members receive access to all submitted Intake Forms. Based on the information in the Intake form, EA and the Navigator/Component Rep may identify and engage SMEs with additional expertise from within CMS.

a) The GRT includes the Navigator/Component Rep, and may also include SMEs from the TRB, Section 508, EA, OAGM, OFM, Capital Planning, Budget, Security and Privacy representatives.

b)

4. The GRT works iteratively to assist the Business Owner in the development of the Business Case. The GRT ensures that the business considers COTS, open source, and new or emerging technologies as potential alternative solutions, and that the business also consider leveraging existing assets and solutions. The Alternatives Analysis within the Business Case compares and contrasts pros and cons for each option. The ISSO should coordinate with the CRA to create an initial Risk Assessment.

a) The role of the GRT is to assist the Business Owner/Component in fully developing the Business Case including an alternatives analysis. The alternatives analysis should include benefit cost analysis as well as the pros and cons from a business, contracts, risk and technology perspective.

b) If GRT SMEs have recommendations, they must be included in the Alternatives Analysis, or justification provided as to why they are not. The GRT SMEs are our internal CMS consultants and consideration of their recommendations must is necessary. If the Business does not agree with their recommendations, they may present other alternatives, but must make the case to the GRB that their Alternative is superior in the listed Pros and Cons.

c) Before moving forward, develop a thorough Business Case and alternatives.

5. The Business Owner and Navigator/Component Rep work with the GRT to finalize the TLC Business Case for the GRB. It is important for the Business Case to contain the alternatives and benefit cost analysis. The Business Owner sends the completed Business Case to the GRT Admin Team, which will review it for completeness, prior to including it on an upcoming GRB meeting.

a) The Business Owner must provide the Business Case far enough in advance for the GRT Admin Team to review and revise if necessary.

6. The Business Owner or Navigator/Component Rep will lead the discussion regarding the Business Case and pros and cons of the proposed solutions. The GRB co-chairs are the CIO, Head of Contracting Activity (HCA), and Chief Financial Officer (CFO), with staff of representatives from the Budget Development Groups (BDGs) and operational areas.

7. The GRB will discuss the identified alternatives and issue their decision indicating which, if any, of the proposed options are in alignment with CMS strategic goals and budget and align with the desired Technical architecture. Acceptance from the GRB means the proposed project/program may be included in the CMS IT Portfolio, making subsequent budget requests or reallocations where necessary. Acceptance from the GRB does not guarantee funding.

Upon selection of one of the acceptable options by the Business Owner, the GRT will issue a Life Cycle ID number that will allow the project to enter the budget and/or acquisition process, as outlined in Appendix B – Capital Planning and Investment Control (CPIC).

C. Information Requirements

1. Business Case

a) The business owner must capture the business need in terms of current organizational gaps and desired solution capabilities to support a business case justification, in compliance with OMB Circular A-130 requirements.
b) Establish a clear Business Case during the Initiate phase.
c) The GRT and the Navigator will assist the business owner in developing a thorough the Business Case prior to submission to the GRB.
d) The Business Owner must send the Business Case to the GRT Admin Team far enough in advance for review and revision if necessary, before being

2. GRB Decision

a) The GRB identifies which of the proposed options is viable based on the alternatives analysis provided by the business owner/project team.

D. Exit Criteria

1. Life Cycle ID Number

a) The GRB has reviewed and approved one or more IT solution approaches that are acceptable to the Business Owner, and issuance of a Life Cycle ID.

E. Roles and Responsibilities

Role	Responsibilities
Budget Development Group (BDG) Representative	• Evaluate the budgetary request and required life cycle investment costs for solution alternatives • Member of the GRB
Business Owner	• Identify and document Business Need • Create Business Case • Present Business Case to GRB meeting • Select an approved alternative for development • Develop Acquisition Plan with OAGM
Capital Planning Analyst	• Identify IT Investment reporting impacts to HHS and OMB. • Assist the Business Owner and Program or Project Manager in updating and creating required capital planning artifacts. • Work with the Business Owner and Program or Project Manager to create board reviewable documents based on the capital planning artifacts. • Work with the Program or Project Manager to update the Portfolio Management Tool to reflect the status of the IT Investment.
Chief Financial Officer (CFO)	• The CMS Chief Financial Officer • Co-Chair of the GRB
Chief Information Officer (CIO)	• The CMS Chief Information Officer, responsible for all IT Investments • Co-Chair of the GRB
Chief Information Security Officer (CISO)	• CMS Chief Information Security Officer • May be represented on the GRB
Component Rep	• The Component Rep could be the Business Owner or designated by the Business Owner, to perform the work of the Navigator if the Component chooses not to use a Navigator.
Cyber Risk Advisor (CRA)	• Monitor Security and Risk of the proposed system alternatives and advise on risk reduction.
Enterprise Architecture (EA)	• Identify potential solution alternatives including any known costs, functional and technical considerations. • Consider impact of integration with interfacing systems.
Governance Review Board (GRB)	• Approve/Deny project to move forward for funding • Authorize proposed approaches or solutions
Governance Review Team (GRT)	• The GRT may consist of SMEs, the TRB, EA, OAGM, OFM, Budget, ISSO, CRA, and PA.

Role	Responsibilities
	• Assist the business owner and Navigator in developing a sound Business Case and Analysis of Alternatives • The GRT Admin Team ensures the alternatives analysis is well developed prior to the GRB meeting • Issue a Life Cycle ID number when the Business Owner has selected an approved alternative solution
Head of Contracting Activity (HCA)	• Director of the Office of Acquisition and Grants Management • Co-Chair of the GRB
Information System Security Officer (ISSO)	• Evaluate information security considerations for proposed solution alternatives. • Provide recommendations during the GRB meeting. • Create a CMS FISMA Controls Tracking System (CFACTS) profile for a new system and initiate the System Security Plan (SSP), or update an existing profile, and support coordination with Information Security governance processes.
Navigator	• Assist the Business Owner in capturing and refining the business need. • Coordinate with SMEs, EA, TRB and other members of the GRT to identify and evaluate solution alternatives • Facilitate the GRB discussion • The Business Owner or a Component Rep must perform these tasks if the component chooses not to have a Navigator.
OAGM Representative	• Evaluate potential procurement approaches for proposed solution alternatives during the GRB.
Privacy Advisor (PA)	• Evaluate privacy considerations for proposed solution alternatives. • Provide recommendations as part of the Governance Review Team.
Section 508 Representative	• Identifies any potential accessisibility issues early on in the developmeent process and shares standards as needed.
SMEs	• Ask questions to clarify business needs • Provide subject matter expertise support to inform solution alternatives
Technical Review Board (TRB) Representative	• Provide inputs into the solution alternatives to ensure alignment with the TRA, CMS Technology Roadmap, and use of new or emerging technologies

F. Related Governance

1. Capital Planning and Investment Control (CPIC)

   Depending on the project size, scope, and priority level, Business Owners will be required to complete additional artifacts in this phase including a Risk Management Plan, Investment Charter, Business Case, Alternatives Analysis, Benefit/Cost Analysis, and Acquisition Strategy (AS).

The business case, alternatives analysis, benefit cost analysis will be utilized by the GRB to properly manage risks and returns during the Select Phase of the CPIC process.

Upon approval and agreement, the Business Owner should complete a preliminary AS with the initial business case and baseline. The AS is a living document that the business owner adjusts as the general business and contracting strategy changes for procuring the assets. The AS is required prior to the Acquisition Plan (AP) for major investments.

An existing investment with major changes may need to update their Acquisition Strategy based on the proposed enhancement/change.

Procurements involving the acquisition of information technology require sign-off from an IT Governance Official. (Send AP to IT_Governance@cms.hhs.gov).

2. Information Security & Privacy

The Business Owner obtains an ISSO for the project, and consults with the CRA to establish the initial Security and Privacy assessment for the proposed system. The CRA assigns a system categorization based on the classification and type of information processed and stored by the solution and the security and privacy risk. Refer to Appendix C – Security and Privacy.

The Business Owner completes a system profile record within CFACTS.

Existing system maintainers shall coordinate with their ISSO to properly document changes to their system and conduct a Security Impact Analysis (SIA) in compliance with CMS Security Policy.

3. Records management and retention schedule

The Office of Strategic Operations and Regulatory Affairs (OSORA) governs Records Management within CMS.

The National Archives (NARA) provides guidelines for the retention of project management documents as well as for records containing business data. Project teams are responsible for maintaining their records in accordance with existing guidelines. NARA's current guidance is located at NARA archives.

IV. Develop Phase

Develop	Update	Key Objectives 1. Identify repository locations for system development artifacts. 2. Satisfy information security, privacy, and Section 508 requirements prior to releasing to the production environment. Exit Criteria 1. Authorization to Operate (ATO) Received. 2. Deploy software solution to the Production environment.

A. Overview

During the Develop Phase, the Developer builds and tests a working solution ready to deploy into the Production environment for operations. The solution must comply with the CMS Technical Reference Architecture as well as policies concerning Information Security, Privacy, and Accessibility (Section 508).

The Target Life Cycle does not specify a development methodology or processes to use as long as they meet the requirements. The chosen Systems Development Life Cycle Methodology best practices will guide the Program Team with processes and artifacts agreed to between the Contractor and the Business Owner.

The Business Owner, or a CMS delegate, has the ultimate responsibility for monitoring development activities, following Best Practices, and complying with IT governance.

B. Information Requirements

Project teams are required to produce and make available to all CMS personnel (not just Contractor personnel) the following artifacts. This policy does not specify a repository to use. A general statement (such as "JIRA") is acceptable during the Initiate phase. When Development begins, the Project Team provides the navigation path to the for audit purposes. CMS prefers that these artifacts be stored on CMS infrastructure to avoid loss when contractors turn over.

- Business Artifacts – Any governance-related artifacts that document program decisions, such as Alternatives Analysis. Additionally, negotiated agreements between the program and service partners, including Contractors, CMS service providers (e.g. Infrastructure, Hosting Providers) and Government Partners, such as Interface Control Documents (ICDs), Data Usage Agreements (DUAs), Memorandums of Agreement (MOA), and Service Level Agreements (SLAs).
- Requirements – Detailed User stories or functional specifications of the desired solution.
- Design – The solution design should include solution architecture and interface control diagrams. This may be the System Design Document (SDD) as required by CFACTS.
- Source Code – Developed software code, including any configuration files, to support the installation and operations of the information system.
- Testing – The Test Plan and reports of results that indicate that the system fulfills the requirements, and complies with CMS Technical standards and Information Security and

Section 508 requirements. The contractor must provide updated reports and results from QA/QC activities with each release.

- Operations & Maintenance (O&M) – Periodic updates to the operational guide for the IT solution, including installation, failover and restoration guides, and system changes.

Business and program teams must be able to provide the documents/artifacts that support their system within two business days, upon request, to fulfill review or audit requests from outside agencies such as OIG and GAO. Failure to comply with requests for documentation may result in negative audit findings and increased scrunity from auditor.

C. Exit Criteria

1. Authorization to Operate (ATO)
   a) The ATO signifies that the system complies with Information Security and Privacy requirements.
   b) The CISO grants the ATO.

2. Successful Testing
   a) Documentation that the system has successfully passed required functional, User Acceptance, and accessibility testing.

D. Roles and Responsibilities

Role	Responsibilities
Business Owner/Proxy	• Responsible for development and creation of Business Case and Analysis of Alternatives. • Implements administrative functions including acquisition, budget, and investment reporting. • Monitors development activities and compliance with IT governance policies. • Adopts and follows a suitable System Development Life Cycle Methodology • Participates in requirements definition and design reviews of the IT solution.
Capital Planning Analyst	• Work with the Program or Project Manager to update the Portfolio Management Tool to reflect the status of the IT Investment. • Assists the P/PM in informing, updating, and completing required artifacts.
Chief Information Security Advisor (CISO)	• Evaluates Systems for qualifications for ATO
Cyber Risk Advisor	• The CMS employee who monitors the system's CFACTS compliance and acts as a liaison for Security issues with the ISSO.
Program Team	• Supports administrative functions including acquisition, budget, and investment reporting. • Defines, designs, develops, tests, and implements IT solution.
Section 508 Representative	• Work with the Program teams to verify that the application complies with Section 508 accessibility requirements and determine if application meets CMS' Exception criteria.
TRB	• The Technical Review Board provides consultative and formal review services to CMS Program teams in order to shape technology decisions to align with the CMS Technical Reference Architecture and Technology Roadmap.

E. Related Governance

1. Capital Planning and Investment Control (CPIC)

   During the develop phase of the TLC, the P/PM should be updating the Portfolio Management Tool for major investments (i.e., Investments over the $10 million threshold). Depending on the size, scope, and priority of the investment, the P/PM will be responsible for updating CMS and HHS leadership, as well as OMB and the public on

cost and schedule milestones of the project(s), performance metrics, and certain artifacts upon request.

Find more information in Appendix B - CPIC - Investment Management/Budget and Acquisition

2. Information Security & Privacy

   The CMS Authorization to Operate (ATO) must be in effect prior to deployment of a new system into production.

   The Project Team must perform the following activities in order to receive an ATO:

   a) Provide a detailed description, in CFACTS, of the system's boundaries and technical components including a combination of network/boundary drawings, hardware and software inventories, and a narrative explaining what is within the boundary.

   b) Finalize the required security and privacy artifacts (ISRA, PIA, CP, CP Testing, SSP etc.).

   c) Conduct Penetration Testing and Adaptive Capabilities Testing (ACT) or Security Control Assessment (SCA).

   d) Mitigate findings from the testing or create POA&Ms prior to Production Deployment.

   e) Submit ATO Certification Form for CISO signature.

   For existing systems, the Project Team must maintain the ATO and ensure all related security activities are completed (e.g. annual Contingency Plan tabletop test, annual review of documentation, etc. for existing systems undergoing changes).

   The Project Team assesses security compliance with every production release for existing systems, using the System Impact Assessment (SIA). To ensure following of all CMS security procedures, project teams must work with their ISSO and CRA.

   Accessibility – The project team must complete and document Section 508 testing as part of the ATO.

3. Records management and retention schedule

   OSORA governs Records Management within CMS.

   The National Archives (NARA) provides guidelines for the retention of project management documents as well as for records containing business data. Project teams are responsible for maintaining their records in accordance with existing guidelines. NARA's current guidance is available here NARA Archives.

V. Operate Phase

Operate	1. Key Objectives 2. Maintain solution availability and performance. Exit Criteria 1. Decommission Decision.

A. Overview

The Operate Phase inititates immediately upon deployment of the solution to the Production environment. The Operate Phase includes O&M activities that refer to operating and maintaining an IT asset that is in a production environment. O&M activities include those associated with sustaining the IT asset at the current capability and performance levels. O&M costs can include Federal and contracted labor, corrective hardware and software maintenance, voice and data communications maintenance and service, replacement of broken or obsolete IT equipment, overhead costs, business operations and commercial services costs.

The project team manages the ongoing operations and maintenance of the solution applying routine maintenance and security practices. Most projects will simultaneously have a production instance (in the Operate Phase) while they continuously work on new functionality or enhancements to their production application in a lower environment (in the Develop Phase).

Business and project teams must maintain the current documentation that is accessible to support internal reviews and audits from outside agencies. The inability to produce current documentation may affect a system's ATO.

B. Information Requirements

1. Ongoing Production Release

   Maintain the Authorization to Operate (ATO) – The project team must work with their ISSO and CRA to ensure adherence to all security standards.

C. Exit Criteria

1. Disposition Decision and Date

   The formal decision by the Business Owner to decommission the solution, and a high-level approach to timeline for shutting down the solution.

D. Roles & Responsibilities

Role	Responsibilities
Business Owner	• Implements administrative functions including acquisition, budget, and investment reporting • Evaluates the continued utility and cost effectiveness of the solution • Monitors partner service level agreements (SLAs) and memorandums of agreement (MOAs) • Sets a date for decommissioning when required
Capital Planning Analyst	• Assists the P/PM to update the Portfolio Management Tool to reflect the status of the IT Investment. • Assists the P/PM in informing of, updating, and completing, required artifacts.
Program Team	• Supports the Business Owner in administrative functions including acquisition, budget, and investment reporting • Supports ongoing operations and maintenance of the operational software and the infrastructure the solution is running on.
TRB	• Provides consultative services, as requested, to the programs to shape technology decisions to align with the CMS Technical Reference Architecture and Technology Roadmap

E. Related Governance

1. Capital Planning and Investment Control (CPIC)

During this phase, OMB requires the P/PM to identify lessons learned and emerging gaps in functionality, performance, or opportunities to improve the current state and submit them upon request.

2. Information Security

The Business Owner/System Maintainer must maintain the CMS ATO and complete all related security activities (e.g. annual Contingency Plan tabletop test, annual review of documentation, etc.). CMS expects the Project Team to maintain the Privacy Impact Assessment (PIA), including any periodic reviews and updates, manage security and privacy risk within an acceptable risk tolerance, and maintain their SORN (System of Records Notice), if applicable.

3. Records Management

The Office of Strategic Operations and Regulatory Affairs governs Records Management within CMS. The National Archives (NARA) provides guidelines for the retention of project management documents as well as for records containing business data. Project teams are responsible for maintaining their records in accordance with existing guidelines. NARA's current guidance is available at NARA archives.

VI. Retire Phase

Retire	CHECKLIST	Key Objectives 1. Archive any data according to the SORN, if present, or other Federal regulation. 2. Close out all related contractual actions and agreements related to the system. 3. Properly dispose of hardware or infrastructure used by the system. Exit Criteria. 1. Business Owner Attestation.

A. Overview

In the Retire Phase, the Project Team discontinues operating the system and performs extensive planning to define all the tasks that are necessary to decommission the system. The TRB provides Disposition Guidance to help project teams plan the disposition of technical elements. They are also available to provide individualized help with disposition requirements and process and completing the Disposition Checklist.

Most projects will simultaneously be in the O&M (Operations Phase) continuously working on current operations as well as a decommissioning strategy and tasks (Retire Phase).

B. Information Requirements

1. Disposition Checklist

A checklist which identifies the activities and processes needed to dispose of a system and its associated hardware and data.

a) Data Center configuration items
b) User accounts, developer accounts, Firewall, security configurations, etc.
c) Archive data, system documentation and software
d) End/return software license agreements
e) Close all CFACTS findings
f) Submit Disposition Memo to the CISO
g) Close out contract/acquisition activities
h) Close out Investment tracking in PMT

C. Exit Criteria

1. Disposition Checklist

D. Roles and Responsibilities

Role	Responsibilities
Business Owner	● Develops and completes the disposition checklist ● Attests to its completion and deliver to Governance
Capital Planning Analyst	● Works with the P/PM to ensure the CMS IT Portfolio changes are completed and the investment is eliminated.
Cyber Risk Advisor	● The CMS employee who monitors the system's CFACTS compliance and acts as a liaison for Security issues with the ISSO
ISSO	● Support disposition activities
Program Team	● Support disposition activities
TRB	● Provide consultative services , as requested, to the programs to ensure an orderly and complete system disposal.

E. Related Governance

1. Information Security

The System Maintainer must complete the Disposition section details within CFACTs and close the project so it is no longer reported as a FISMA system in CFACTs.

Completion of disposition documentation, which includes:

- The Federal Information Security Management Act (FISMA) System Retirement Memo
- System Disposition Plan and Report
- Destruction Certification

VII. Available CMS Resources

A. Delegation of governance functions.

The CIO may delegate responsibility for the preparation and oversight of governance functions to existing boards which have sufficiently developed support processes to facilitate the TLC processes for their investments. This delegation does not remove the responsibility of the component to present the required Business Case with proposed alternatives, initial investment requested, and major changes to the GRB for review and approval, as well as to comply with CMS technical, security and privacy requirements.

B. Governance Review Team (GRT)

The GRT consists of representatives from investment management (CPIC), Technical Review Board, EA, IT Budget, infrastructure, Security, Privacy, Section 508, navigator program, shared services, and data.

The main roles of the GRT are:

- To assist the Business Owner in developing a meaningful Business Case
- To assist the Business Owner and Navigator in developing Pros and Cons for the potential solutions identified by EA
- To review the Business Case before presentation to the GRB
- To provide ongoing review of proposed and operational systems for adherence to CMS policies
- To invoke situational reviews by the TRB or GRB, EA consults, and TechStat reviews when necessary and/or triggered by changes in the TLC System Profile

C. TRB Engagements

Throughout the Target Life Cycle, the TRB is available to programs to provide input and shape solutions to better align with CMS Technical Reference Architecture and best practices. The TRB is available to conduct situational reviews as determined by the GRT, TRB or other governance body. The TRB also provides formal and informal technical consultations at any point in the life cycle of a program.

D. EA Consult

The EA team is responsible for managing the EA repository, which houses critical IT solution information to support audit and reporting activities. Additionally, the EA team will support early IT solution discussions to identify and evaluate potential solution alternatives, including existing CMS solutions and Government-Off-The-Shelf (GOTS) solutions, and align solutions against CMS Technical Reference architecture and standards. EA is also available to support for situational reviews as determined by the GRT.

VIII. Appendix A - Required Artifacts

Artifact	Purpose	Justification
Business Case	Describes the basic aspects of the proposed IT project: why, what, when, and how.	OMB Circular No. A-130, FITARA
Alternatives Analysis	The Business Case includes varying approaches to fulfilling the same business need which the GRT/GRB compare to determine optimal solutions.	OMB Circular No. A-130, FITARA
Enterprise Architecture Profile	Consists of models, diagrams, tables, and narrative, which show the proposed solution's integration into CMS operations from both a logical and technical perspective.	OPEN Government Data Act of 2017, E-Government Act of 2002
Technical Design	Describes the technical aspects of the system and how it integrates with the CMS architectural standards.	E-Government Act of 2002, Clinger-Cohen Act of 1996
Source Code	Ensures that transition to a different contractor will not cause loss of CMS asset.	NA
Requirements/User Stories	Identifies the business and technical capabilities and constraints of the IT project.	E-Government Act of 2002
Test Plans, Defect/bug and Test Summary Reports	Describes the overall scope, technical and management approach, resources, and schedule for all intended test activities associated with validation testing: reports summarize test activities and results including any variances from expected behavior.	E-Government Act of 2002
Section 508 Compliance	Indicates system compliance with 508 standards and guidelines	FISMA, OPEN Government Data Act of 2017
User Guide and Training Materials	Explains how a novice business user is to use the automated system or application from a business function perspective.	The Paperwork Reduction Act of 1995 (PRA) / 44 U.S.C. 3506
Operations and Maintenance Guide	Guides those who maintain, support and/or use the system in a day-to-day operations environment. Ensures that transition to a different contractor will not cause loss of CMS asset.	E-Government Act of 2002, Clinger-Cohen Act of 1996

Artifact	Purpose	Justification
Authorization to Operate (ATO) Investment Management/Budget & Acquisition	Demonstrates and validates that appropriate security controls exist to safeguard the system. Provides CIO approval of System Certification and System Accreditation authorizing the system to become operational.	FISMA

IX. Appendix B – Capital Planning and Investment Control (CPIC)

The Clinger-Cohen Act (CCA) of 1996 (Division E of Public Law 104-106, formerly known as the IT Management Reform Act of 1996) requires federal agencies to use a disciplined CPIC process to acquire, use, maintain and dispose of IT assets. Other laws and policies, such as the Paperwork Reduction Act of 1980 and 1995, the Government Performance and Results Act of 1993, the Federal Acquisition Streamlining Act of 1994, the Federal Information Technology Acquisition Reform Act of 2014, and OMB Circular A-130, Management of Federal Information Resources, also require agencies to design and implement a disciplined process to maximize the value and assess and manage IT Investment risks.

CCA mandates that the CPIC process shall:

1) Provide for the selection, control, and evaluation of agency IT Investments;
2) be integrated with the processes for budget, financial, and programmatic decision-making;
3) include minimum criteria for considering whether to undertake an IT Investment;

identify IT Investments that would result in shared benefits or costs for other Federal agencies or State or local governments;

4) provide for identifying quantifiable measurements for IT Investment net benefits and risks;
5) provide the means for senior management to obtain timely information regarding an Investment's progress.

b)

CPIC is a management process for ongoing identification, selection, control and evaluation of investments in information resources. It is a continuous and integrated process for managing the risks and returns of IT Investments. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes. The TLC, CPIC and Project Management best practices are interwoven within IT solution implementation. This process helps ensure that CMS develops and maintains a sound IT Portfolio.

Depending on the investment classification (e.g. Major, Standard, or Non-Major), the program or project manager (P/PM) must still adhere to certain IT Capital Planning requirements as established by HHS and the Office of Management and Budget. These policies help ensure compliance with legislative and regulatory requirements. The P/PM should include someone from the CPIC Investment Management team within the integrated project team (IPT). This person will help ensure that the rest of the IPT is aware of any reporting requirements related to the project and/or program.

The CPIC process is always ongoing and consists of three phases: Select, Control, and Evaluate. Each of these phases can also be broken down into additional sub phases to better understand the purpose and functions.

The Business Owner justifies the investment during the Select Phase, which coincides with the TLC Initiate phase by developing a business case, project management plan, risk management plan, investment charter, acquisition strategy, and alternatives analysis. For iterative methodologies, this may also include a release plan, sprint plan with backlog and burn down

chart, and/or a product backlog. The GRB utilizes the business case and alternatives analysis to determine if the project should be included in the CMS IT portfolio and thus funding requested for it. OAGM utilizes the acquisition strategy to determine if the overall approach to acquiring the assets make sound business sense and thus further acquisition planning (development of the acquisition plan) may take place. Approval of the strategy will allow the Project Team to move forward into the develop phase of the TLC.

The Control Phase of CPIC, primarily coincides with the develop phase of the TLC, but also the operate phase. During this phase, the OMB imposes sound project management practices on selected investments to ensure they are on schedule, within budget, and meeting the scope of work. OMB his is typically done through periodic reviews such as an operational analysis and post implementation review. CMS CIO collects IT investment information about these two processes from the P/PMs and submits to OMB upon request.

The Evaluate phase of the CPIC process consists of annual evaluations (operational analysis) as well as post implementation reviews (review immediately following project completion). The project teams conducts the post implementation reviews or PIRs within the first 6 months of project completion to identify lessons learned. The project team also conducts annual evaluations to identify emerging gaps in functionality, performance, and modify investments as necessary. The operational analysis is a valuable tool that can help ensure PMT reporting and GPR updates are made timely in order for leadership to make well informed data driven decisions.

X. Appendix C – Security and Privacy

The Key Enterprise System Security Lifecycle (KESSeL) roadmap and checklist, are convenient tools to guide the Business Owner and ISSO through the security and privacy steps of the TLC.

These tools are available on the Information Security and Privacy Library.
https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library

The Information Security & Privacy Group (ISPG) Advantage

Forging a strong partnership with your designated ISPG Advisors will help you navigate smoothly throughout all of the phases of the TLC. Engaging early and often with your Cyber Risk and Privacy Advisor will allow you to plan appropriately and design resilient systems and programs that reduce risk and cost less. Here is what ISPG's Portfolio Program can do for you:

Who are the key stakeholders?

- Cyber Risk Advisor
- Privacy Advisor
- Information System Security Officer
- Business Owner
- System Owner

What services does ISPG offer?

- DevSecOps Pipeline
- ISSO as a Service
- SOC as a Service / CDM Integration
- PenTest as a Service
- PrivacyOps Engineering (other options: Privacy Continuous Monitoring, PrivacybyDesign or Transparency is the new Privacy)

What's the value proposition of leveraging ISPG's offerings?

- Authority to Operate process comes first
    - All the changes are captured in a consistent development environment
    - Reduces the need to accept risk at go-live
- Eliminates extraneous or redundant deployment of tools
- Improves visibility & Reduces risk
- Streamlines governance & Centralizes monitoring
- Intelligent consolidation of resources across the enterprise

XI. Glossary and Guide to Acronyms

Acronym	Term	Definition
AS	Acquisition Strategy	The AS is a strategic document with sufficient detail to enable senior leadership and other decision authorities to assess whether the strategy makes good business sense, effectively implements laws and policies, and reflects management's priorities, before allowing the Program/Project (P/P) to proceed to the next phase of the acquisition life cycle. Once approved, the AS provides a basis for more detailed planning.
ATO	Authority To Operate	The ATO process is an essential part of the CMS enterprise-wide Information Security Program. The CISO uses this information to make a risk determination decision for the operation of the subject system. When the CISO deems the level of risk is acceptable to CMS, the CIO grants an ATO for up to three years.
BC	Business Case	A business case outlines a justification for a proposed project on the basis of its expected impact on the strategic goals of CMS, why and what the business need is, the expected benefits, and potential alternative solutions with broad estimates of time and cost.
BO	Business Owner	The Business Owner (BO) is the executive in charge of the organization who serves as the primary customer and advocate for an IT project. The BO is responsible for identifying the business needs and performance measures to be satisfied by an IT project; providing funding for the IT project; establishing and approving changes to cost, schedule, and performance goals; and validating that the IT project initially meets and continues to meet business requirements.
CFACTS	CMS Federal Information Security Management Act Controls Tracking System	CFACTS is the CMS Governance, Risk and Compliance tool used as a repository to manage the security and privacy requirements of its information systems. This platform provides a common foundation to manage policies, controls, risks, assessments and deficiencies across the CMS Enterprise.
-	CMS System Census	The EA enumeration of IT systems within CMS and relevant characteristics about them.

Acronym	Term	Definition
CPIC	Capital Planning and Investment Control	Capital Planning and Investment Control (CPIC) is a management process for ongoing identification, selection, control and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes
CRA	Cyber Risk Advisor	ISPG member who facilitates and oversees the completion of all federal cybersecurity and privacy requirements
-	Disposition	Disposition is the process of retiring a capital asset once its useful life is completed or a replacement asset has superseded it. Business Owners may include disposition costs in the operational activities near the end of the useful life of an asset.
DME	Development, Modernization, and Enhancement	DME refers to projects and activities leading to new IT assets/systems, as well as projects and activities that change or modify existing IT assets to substantively improve capability or performance, implement legislative or regulatory requirements, or meet an Agency leadership request. DME activity may occur at any time during a program's life cycle. As part of DME, capital costs can include hardware, software development and acquisition costs, commercial off-the-shelf acquisition costs, government labor costs, and contracted labor costs for planning, development, acquisition, system integration, and direct project management and overhead support.
EASI	Easy Access to System Information	Components use EASI supports the IT Intake process and captures Business Case documentation and distribution for projects going through the TLC Governance process. EASI is a resource channel for CMS internal stakeholders to access CMS systems information on a single platform and allow stakeholders to easily find information at a high level and access other channels for more detailed features.

Acronym	Term	Definition
EA	Enterprise Architecture	EA is a management engineering discipline presenting a comprehensive view of the enterprise, including strategic planning, organizational development, relationship management, business process improvement, information and knowledge management, and operations. EA consists of models, diagrams, tables, and narrative, which together translate the complexities of the agency into simplified yet meaningful representations of how the agency operates (and intends to operate). EA may also refer to the team or person, which performs this job within CMS.
FISMA	Federal Information Security Management Act	FISMA is a United States federal law passed in 2002 that made it a requirement for federal agencies to develop, document, and implement an information security and protection program. FISMA is part of the larger E-Government Act of 2002 introduced to improve the management of electronic government services and processes.
ISSO	Information System Security Officer	ISSOs are the project based managers of the technical and business processes for securing information and systems based on the assessed risks and identified risk tolerance. The Business Owner of a system designates the ISSO.
GRB	Governance Review Board	The CMS GRB is the executive review and decision-making body for CMS IT portfolio management. The goal is to provide enterprise-wide strategic decision-making, shared leadership, transparency, monitoring, and true ownership of major IT investment decisions, opportunities and risks. The GRB will review and approve IT initiatives, expenditures, and capital plans. It will ensure that proposed investments contribute to the Secretary's strategic vision and mission requirements, meet the business needs of the Agency, employ sound IT investment methodologies, comply with Departmental systems architectures, and provide the highest return on investment and mitigate project risk.

Acronym	Term	Definition
GRT	Governance Review Team	The GRT consists of representatives from the following areas: TRB, EA, Investment Management, Acquisitions and Contracts, Financial Management, Infrastructure, Security and Privacy, Section 508, Shared Services, and Data. The GRT may pull representatives from other areas as needed. The GRT analyzes the project information and advises project teams on how to proceed through the CMS IT Governance process, what resources are available to help, and how to properly develop and document their IT project Business Case and Alternatives Analysis.
IaaS	Infrastructure as a Service	A form of cloud computing that provides virtualized computing resources over the internet. IaaS is one of the three main categories of cloud computing services, alongside software as a service (SaaS) and platform as a service (PaaS).
-LCID	Life Cycle ID number	CMS IT Governance issues Life Cycle IDs (LCIDs) for each new Acquisition Plan and each new IT development effort, which demonstrates compliance with CMS' IT Governance process. The CMS IT Governance Admin team evaluates any planned contract actions or changes to systems using trigger thresholds that indicate additional review is necessary.
NARA	National Archives and Records Administration	The agency of the United States government charged with preserving and documenting government and historical records and with increasing public access to those documents.
-	Navigator	An OIT employee who can connect you with the right resources, people and services that you need to accomplish your component's business objectives, and guide you and your request through the process until completion, keeping you informed of the status along the way.

Acronym	Term	Definition
O&M	Operations and Maintenance	OMB Capital Planning Guidance defines Operations and Maintenance as activities necessary to keep an asset functioning as designed during the O&M phase of an investment. These activities include, but are not limited to operating system upgrades, technology refreshes, security patch implementations, activities that operate data centers, help desks, operational centers, telecommunication centers, and end-user support services. Activities that expand the capacity of an asset or otherwise upgrade it to serve needs different from or significantly greater than those originally intended are DME.
-	Material Change	A change to system characteristics that may trigger a governance or security review. A material change may differ from project to project depending on context.
PaaS	Platform-as-a-Service	A cloud computing model in which a third-party provider delivers hardware and software tools to users over the internet. A PaaS provider hosts the hardware and software on its own infrastructure. As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application. PaaS is one of three main categories of cloud computing, alongside infrastructure as a service (IaaS) and Software as a service (SaaS).
PA	Privacy Advisor	ISPG member who provides privacy-related expertise to help the team identify and manage privacy risk.
SaaS	Software as a service	A software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet. SaaS is one of three main categories of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS).
Section 508	Section 508 Compliance	Section 508 of the Rehabilitation Act requires that institutions receiving federal funds solicit, procure, maintain and use all Information and Communication Technology (ICT) so that equal or alternate/comparable access is given to federal employees and members of the public with and without disabilities.

Acronym	Term	Definition
SORN	System of Record Notice	The Privacy Act requires that a notice describing each system of records proposed for establishment by a Federal agency be published in the Federal Register for review and comment by the public and other interested parties. This allows interested parties to raise questions before the system is put into effect while also ensuring the Project Team addresses all privacy considerations.
SSP	System Security Plan	The purpose of a System Security Plan (SSP) is to provide an overview of the security requirements of a system and describe the controls that are in place or planned to meet those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system.
TLC	Target Life Cycle	The TLC is the Governance Framework developed by CMS to promote compliance with IT Investment oversight and governance standards while remaining flexible and proportional. The TLC GRT will perform continuous monitoring and evaluation and utilize situational reviews when necessary.
SME	Subject Matter Expert	A person who has an in-depth knowledge of a particular topic, which is part of the subject at hand.
TRA	Technical Reference Architecture	The CMS Technical Reference Architecture provides CMS's authoritative technical architecture approach and technical reference standards to assure the secure and high-quality delivery of healthcare services to beneficiaries, providers, and business partners. The TLC requires all agency business partners in developing, transitioning to, and maintaining CMS Processing Environments. *Note: The five volumes of the TRA are available on the CTO Corner TRA SharePoint site. This is an internal CMS website that is not available to the public. Business partners, who require these documents but do not have access to the site, should contact their CMS project manager/project lead or Contracting Officer's Representative (COR) for a copy.*
TRB	Technical Review Board	The CMS technical governance body for IT projects that provides guidance to project teams on adhering to CMS technical standards and leveraging existing technologies (e.g., Shared Services).