



CMS Target Life Cycle

Overview

July 12, 2019

Table of Contents

The CMS Target Life Cycle (TLC).....	3
I. Executive Summary	3
A. Initiate Phase	4
B. Develop Phase	4
C. Operate Phase	4
D. Retire Phase.....	4
E. Available Resources.....	4
F. Capital Planning Investment Control and Security Assessment and Authorization	4
II. Initiate Phase	5
A. Overview	5
B. Initiate Phase Detailed Flow	6
C. Information Requirements	8
D. Exit Criteria	8
E. Roles and Responsibilities.....	8
F. Related Governance.....	10
III. Develop Phase	12
A. Overview	12
B. The Governance Profile Repository (GPR)	12
C. Information Requirements	13
D. Exit Criteria	14
E. Roles and Responsibilities.....	14
F. Related Governance.....	15
IV. Operate Phase	17
A. Overview	17
B. Information Requirements	17
C. Exit Criteria	17
D. Roles & Responsibilities	18
E. Related Governance.....	18
V. Retire Phase.....	19
A. Information Requirements	19
B. Exit Criteria	19
C. Roles and Responsibilities.....	20

D. Related Governance..... 20

VI. Available CMS Resources 21

 A. Delegation of governance functions. 21

 B. Governance Review Team (GRT) 21

 C. Technical Review Board (TRB) Consult..... 21

 D. TLC Resource Library 21

 E. Enterprise Architecture (EA) Consult 21

VII. Appendix A - Required Artifacts..... 22

VIII. Appendix B – Monitored Fields 23

IX. Appendix C – Capital Planning and Investment Control (CPIC)..... 25

X. Appendix D – Security and Privacy 27

XI. Appendix E - TLC Project Worksheet..... 29

XII. Glossary and Guide to Acronyms..... 35

DRAFT

The CMS Target Life Cycle (TLC)

I. Executive Summary

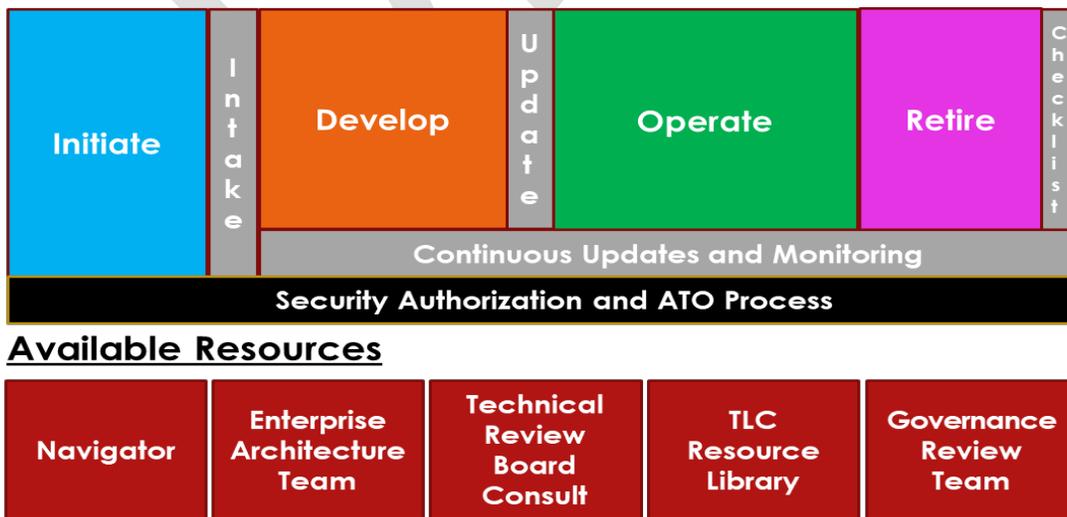
The Centers for Medicare & Medicaid Services (CMS) is committed to empowering business flexibility in IT system development, making sound investment decisions, and complying with Federal IT laws and regulations. Prior governance has relied on extensive, rigidly formatted documentation and gate reviews. 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. The four phases of the TLC are illustrated in Figure 1.

Key Concept #1: System Profile - Key system characteristics will be tracked in a system profile using the Enterprise Architecture (EA) CMS System Census data as the foundation. Select Security and Budget information will complete the profile, with that data being pulled from the corresponding source systems. The system profile will be reviewed and updated prior to every system release to ensure that any future changes are reflected prior to the changes being implemented into production.

Key Concept #2: Situational Governance - Changes to the system profile will allow CMS to apply situational governance commensurate and specific to the changes being made. This new approach will allow for the least possible governance overhead while still ensuring that CMS systems are securely developed and properly supported. CMS will also employ ongoing monitoring of CMS systems to ensure that the system profiles are being accurately maintained.

The Business Owner is responsible for ensuring that the System Maintainer has adopted and is complying with a suitable Systems Development Methodology for documenting requirements, development, and testing of the solution, as well as managing risk. Governance will not be reviewing those artifacts on an ongoing basis, but they must be available to satisfy internal and external audits.

Figure 1. CMS Target Life Cycle Phase Summary



A. Initiate Phase

The purpose of the Initiate Phase is to document the general business need and to provide the Business Owner with acceptable solution alternative(s) which address the business need, optimize integration with external systems, and represent sound investment decisions. This process will rely heavily on the Business Owner, the EA team, Navigator, Subject Matter Experts (SMEs), and the Governance Review Team (GRT) to develop, document, and evaluate potential options for development. Representatives from Security, Privacy and Accessibility must be consulted by the project 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. Requirements, user stories, design, development and testing must all be done in compliance with the CMS Technical Reference Architecture (TRA) and security, privacy and accessibility standards.

The system development methodology is not prescribed, but must be established by the Business Owner and Developer. The TLC requires only a minimal set of artifacts, but components are expected to conform to their chosen system development methodology and to follow best practices in Program Management.

C. Operate Phase

The purpose of the Operate Phase is to maintain steady Production operations while ensuring that routine maintenance is performed and sound security practices are maintained. COTS upgrades, system software patches, hardware upgrades, and modifications to interfaces with other systems are all maintenance issues that must be supported throughout 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

There are additional resources available for the project team to engage if additional information or guidance is needed or a situational review is triggered by [Governance Profile Repository](#) (GPR) updates.

F. Capital Planning Investment Control and Security Assessment and Authorization

The TLC requires a fully vetted CMS Authority to Operate (ATO). All CMS ATO processes and procedures must be followed 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.

II. Initiate Phase

Initiate	Intake	Key Objectives
		Exit Criteria

1. Clarify business needs
2. Evaluate solution alternatives
3. Establish initial GPR entry

1. The Business Case and Analysis of Alternatives have been documented in the TLC Project Worksheet
2. An approved solution has been selected by the Business Owner
3. A Lifecycle ID number has been issued.

A. Overview

All new business needs and material changes to existing systems must go through the Initiate phase. Business needs must be documented, and alternative solutions must be considered, 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, TRA, and existing assets in order to define and document the general business need or enhancement, and explore and document solution options. Cloud Computing, i.e.: Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and Infrastructure-as-a-Service (IaaS) solutions should be considered, and a determination made if existing CMS/HHS vehicles can be leveraged. An ISSO and CRA must be assigned at this stage, to make an initial assessment of security risks and privacy considerations.

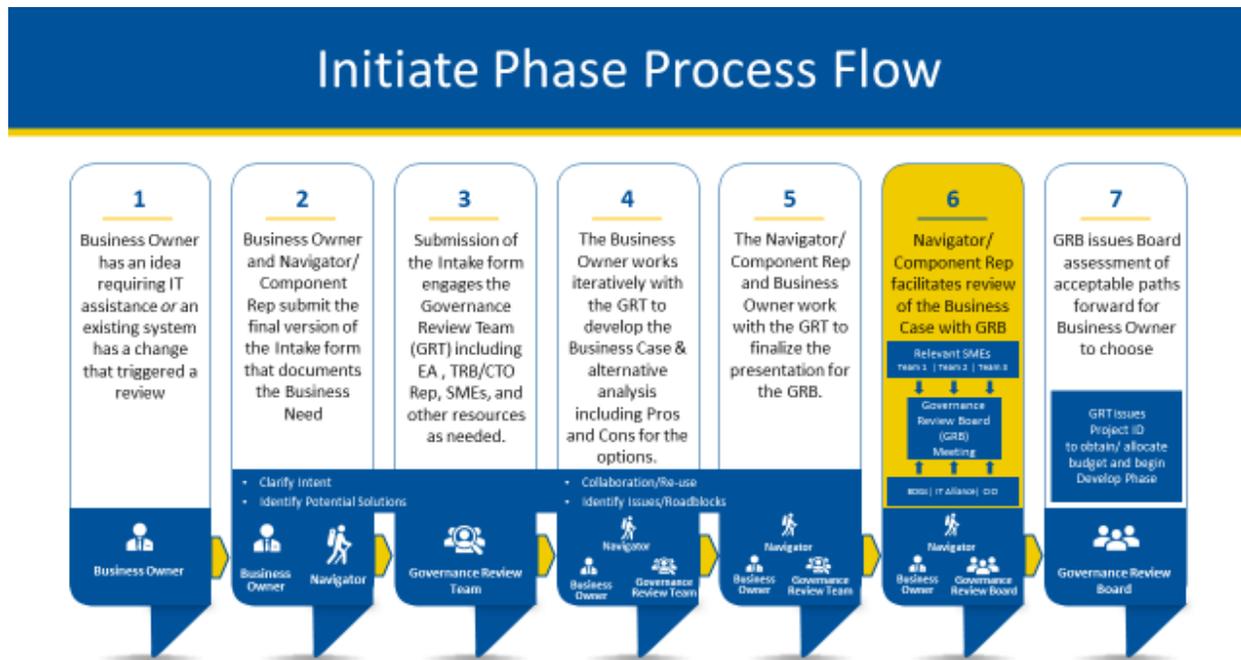
Collaboration with the SMEs and EA to develop and document the business need, recommended alternatives, and recommended budget is an iterative process. There is no specific order and often the business needs become clearer and gain detail after multiple rounds of discussion and questions. The requirement is that the Business Owner provides a fully developed business case prior to the Governance Review Board (GRB) meeting.

The Governance Review Board (GRB), consisting of the CMS Chief Information Officer (CIO), Chief Info Security Officer (CISO), IT Alliance, Budget Development Group (BDG), and SMEs will evaluate the potential solutions to ensure that informed investment decisions are made 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 Governance Review Board, the Business Owner will engage the relevant components to arrange any necessary funding and contract actions before proceeding to the next phase, Develop.

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 starts 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.
 - a) Business components which do not have a Navigator may request that a Navigator from the Office of Information Technology (OIT) be assigned to their project.
 - b) If a Navigator is not requested/needed, 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.

3. When the Intake form is submitted, the GRT members receive an emailed copy. 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, the TRB, EA, OAGM, OFM, Capital Planning, Budget, Security and Privacy representatives.
4. The GRT works iteratively to assist the Business Owner in the development of the Business Case. EA will coordinate with the Chief Technology Officer (CTO) and Technical Review Board (TRB) to ensure that COTS, open source, and new or emerging technologies are considered as potential alternative solutions, and that existing assets and solutions are leveraged. An alternative analysis must be completed including 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 alternative solutions, which includes 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) The Business Case and alternatives should be well developed before moving forward. Please see Appendix E – TLC Project Worksheet for more detail on the content of a Business Case.
5. The Business Owner and Navigator/Component Rep work with the GRT to finalize the TLC Worksheet presentation for the GRB. It is important for the Business Case to contain the alternatives and benefit cost analysis. The Business Owner sends the completed TLC Worksheet to the GRT in order to be included on an upcoming Governance Review Board (GRB) meeting. The TLC Worksheet must be delivered to the GRT and GRB members prior to the meeting for review.
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 will be comprised of the Budget Development Groups (BDGs), the CMS Chief Information Officer (CIO), CISO and the IT Alliance. The GRB will discuss the identified alternatives and issue their decision indicating which, if any, of the proposed options are acceptable and are in alignment with CMS strategic goals and budget. An approval from the GRB means the proposed project/program will be included in the CMS IT Portfolio and subsequent budget requests can be made. An approval from the GRB does not guarantee that funding will be provided.
7. If the Governance Review Board does not approve any option which satisfies the business need and is acceptable to the Business Owner, the proposal will be escalated to the Information Technology Investment Review Board (ITIRB) for resolution.

Upon selection of one of the approved options by the Business Owner, the GRT will issue a Lifecycle ID number that will allow the project to enter the budget and/or acquisition process, as outlined in [Appendix C – Capital Planning and Investment Control \(CPIC\)](#). The Navigator and Business Owner will create the initial version of the Governance Profile Repository entry for a new system as outlined in [Appendix B – Monitored Fields](#).

C. Information Requirements

1. Business Case - The business need must be captured in terms of current organizational gaps and desired solution capabilities to support a business case justification, in compliance with OMB Circular A-130 requirements. See the template at [Appendix E – TLC Project Worksheet](#).
 - a) A clear Business Case must be established during the Initiate phase. The Business Case should include: the Business Need, legislative mandates or drivers, goals/scope, stakeholders, risks/issues, alignment to strategic objectives, initial performance goals and measures, benefit/cost analysis, and a preliminary acquisition strategy. The GRT and the Navigator will assist the business owner in ensuring the Business Case is well developed prior to submission to the GRB.
 - b) Governance Review Board Decision – indicates which of the proposed options are approved by the Governance Review Board based on the alternatives analysis provided by the business owner/project team.

D. Exit Criteria

1. Lifecycle ID Number - The Governance Review Board was conducted and has approved one or more IT solution approaches that are acceptable to the Business Owner, or the ITIRB has issued approval. A Lifecycle ID number has been issued.
2. Project Initiation – The Business Owner has acquired budget approval and funding for the chosen solution.
3. Initial Governance Profile Repository entry (or updates for an existing system) - The initial record within the Governance Profile Repository has been created for the approved solution, or updates have been completed for changes to an existing system.
 - a) The system characteristics that need to be captured in the Governance Profile Repository are listed in [Appendix B – Monitored Fields](#).

E. Roles and Responsibilities

Role	Responsibilities
Budget Development Group (BDG) Representative	<ul style="list-style-type: none"> ● Evaluate the budgetary request and required life cycle investment costs for solution alternatives ● Member of the GRB
Business Owner	<ul style="list-style-type: none"> ● Work with Navigator to identify and document Business Need ● Create Business Case ● Support Governance Review Board meeting ● Select an approved alternative for development ● Develop Acquisition Plan with OAGM
Capital Planning Analyst	<ul style="list-style-type: none"> ● 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.

Role	Responsibilities
	<ul style="list-style-type: none"> ● 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 current status of the IT Investment.
Chief Information Officer (CIO)	<ul style="list-style-type: none"> ● The CMS Chief Information Officer, responsible for all IT Investments ● Member of the GRB
Chief Information Security Officer (CISO)	<ul style="list-style-type: none"> ● CMS Chief Information Security Officer ● Member of the GRB
Component Rep	<ul style="list-style-type: none"> ● 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 to not use a Navigator.
Cyber Risk Advisor (CRA)	<ul style="list-style-type: none"> ● Monitor Security and Risk of the proposed system alternatives and advise on risk reduction.
Enterprise Architecture (EA)	<ul style="list-style-type: none"> ● Identify potential solution alternatives including any known costs, functional and technical considerations. Consider impact of integration with interfacing systems.
Governance Review Board (GRB)	<ul style="list-style-type: none"> ● Approve/Deny project to move forward for funding ● Authorize proposed approaches or solution(s)
Governance Review Team (GRT)	<ul style="list-style-type: none"> ● The GRT may consist of SMEs, the TRB, EA, OAGM, OFM, Budget, ISSO, CRA, and PA. ● Assist the business owner and Navigator in developing a sound Business Case and Analysis of Alternatives ● Ensure the alternatives analysis is well developed prior to the Governance Review Board meeting ● Issue a Lifecycle ID number when the Business Owner has selected an approved alternative solution
Information System Security Officer (ISSO)	<ul style="list-style-type: none"> ● Evaluate information security considerations for proposed solution alternatives. ● Provide recommendations during the Governance Review Board 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.
Investment Review Board (ITIRB)	<ul style="list-style-type: none"> ● Information Technology Investment Review Board ● The executive review and decision-making body for CMS IT management
Navigator	<ul style="list-style-type: none"> ● Assist the Business Owner in capturing and refining the business need.

Role	Responsibilities
	<ul style="list-style-type: none"> • Coordinate with SMEs, EA, TRB and other members of the GRT to identify and evaluate solution alternatives • Facilitate the Governance Review Board discussion • These tasks must be performed by a Component Rep or Business Owner if the component chooses to not have a Navigator.
OAGM Representative	<ul style="list-style-type: none"> • Evaluate potential procurement approaches for proposed solution alternatives during the Governance Review Board
Privacy Advisor (PA)	<ul style="list-style-type: none"> • Evaluate privacy considerations for proposed solution alternatives. • Provide recommendations as part of the Governance Review Team during the Governance Review Board.
SMEs	<ul style="list-style-type: none"> • Identify questions to clarify business needs • Provide subject matter expertise support to inform solution alternatives
Technical Review Board (TRB) Representative	<ul style="list-style-type: none"> • 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)

Artifacts that may be required (depending on size, scope, and priority of the project) during this phase include the 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. For more information on the CPIC process and its phases, please see [Appendix C – Capital Planning and Investment Control \(CPIC\)](#).

A preliminary AS should be completed with the initial business case. Once a solution is approved and agreed upon, the AS should be baselined. The AS is a living document and should be adjusted as the general business and contracting strategy changes for procuring the assets. The AS will be 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.

More information can be found in [Appendix C - CPIC - Investment Management/Budget and Acquisition](#)

2. Information Security & Privacy

An ISSO must be assigned to the project, and a consultation with the CRA must be held, to establish the initial Security and Privacy assessment for the proposed system. A system categorization must be assigned to the new system based on the classification and type of information processed and stored by the solution. The categorization is based on the security and privacy risk. Refer to [Appendix D – Security and Privacy](#).

Upon completion of the Governance Review Board a system profile record must be established within CFACTS.

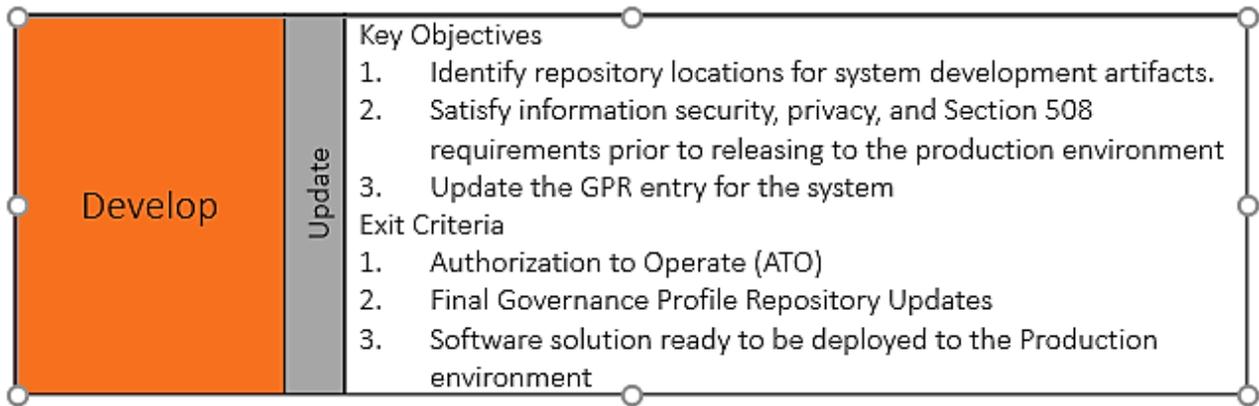
Existing systems shall coordinate with their ISSO to ensure that changes to their system are documented properly in CFACTS and that a Security Impact Analysis (SIA) is conducted in compliance with ISPG Policy.

3. Records management and retention schedule

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 can be found at their [website](#).

III. Develop Phase



A. Overview

During the Develop Phase, a working solution will be developed, built and tested, ready to be deployed 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 what development methodology or processes should be used as long as the requirements are met. The Program Team will be guided by the development methodology, processes, or artifacts agreed to between the Contractor and the Business Owner, while the GRT and the Navigator will assist the Business Owner in ensuring that legal and regulatory requirements for each investment are met.

B. The Governance Profile Repository (GPR)

The establishment of the GPR allows CMS to continuously validate the profile of the application throughout development and operations without requiring structured gate reviews. The GPR consists of key system characteristic values from the CMS System Census performed by EA, as well as data from other CMS systems. These key fields will allow us to have a forecasted vision of the CMS IT infrastructure and allow more informed investment decisions to be made.

For the initial production release, OIT, EA, the Navigator and the Business/Program will together make sure that the entry in the GPR is complete and accurate, to ensure a clear understanding of the profile characteristics being monitored and the expectation of continuing accuracy.

Early entry of changes to this information will allow EA and the GRT to identify any that may require further action before deployment. If proposed changes to the system characteristics or security profile will impact the system such that further governance or security involvement is required, the GRT will coordinate with the stakeholders to mitigate the impact if possible. In order to avoid any impact, any release with GPR changes must update their GPR at least 2 weeks prior to the scheduled deployment. For high impact changes such as migrations or expansion of scope or access

methods, more than 2 weeks advance notice will be required. The project team should notify the GRT as soon as such changes are identified to allow proper planning,

The GRT will conduct continuous monitoring of the GPR against the operational system to validate the accuracy of the data entered by the project team and business owner. Discrepancies in the GPR will result in security findings being entered in CFACTS, unless the project team is able to remediate the discrepancies within a timeframe established based on severity. Multiple or repeat discrepancies will trigger a more in-depth program review to mitigate the failure in program processes and compliance, and to discuss remediation actions.

The Business Owner, or a CMS delegate, has the ultimate responsibility for monitoring development activities and following Best Practices, complying with IT governance, and the accuracy of the GPR data. The GPR data must be kept current and accurate, and updated based on new releases. The Business Owner, or CMS delegate, is encouraged to participate in the Develop Phase activities to more proactively shape the IT solution and provide on-going feedback to the development team(s).

C. Information Requirements

The following [artifacts](#) are required and must be in a form and location which is accessible to CMS personnel (i.e. not just the Contractor personnel). This policy is agnostic as to the repository(s) used but the location must be identified in the GPR by entry of the navigation path to the artifacts. A general statement (such as "JIRA") is acceptable during the Initiate phase, but once the Develop Phase has begun, the actual navigation path linking to those active repositories must be entered in the GPR.

- 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 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. Reports and results from QA/QC activities must be updated with each release.
- Operations & Maintenance (O&M) – Operational guide for the IT solution, including installation, failover and restoration guides, which should be periodically updated as changes are made to the system.

Business and program teams must be able to provide the documents/artifacts that support their system within 2 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 will result in findings entered into CFACTs that will go against the system ATO. This will be in addition to the increased scrutiny that will be applied as a result of the audit itself.

The TLC is a new process and we need the cooperation of all components in order to be successful and mitigate previous audit findings against CMS. 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 to be added to the TLC lifecycle, stored and retained centrally,.

D. Exit Criteria

1. Authorization to Operate (ATO) – The ATO signifies that the system complies with the CMS Technical Reference Architecture, and Information Security, Section 508, and Privacy requirements. The ATO is granted through the Chief Information Officer (CIO).
2. GPR Update – The GPR must be updated to accurately reflect the production profile of the system, whether it is the initial release or a change to an existing system. The system characteristics that need to be tracked are listed in [Appendix B – Monitored Fields](#).

E. Roles and Responsibilities

Roles	Responsibilities
Business Owner/Proxy	<ul style="list-style-type: none"> • 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. • Ensures that a suitable System Development Lifecycle methodology is adopted and followed. • Participates in requirements definition and design reviews of the IT solution.
Cyber Risk Advisor	The CMS employee who monitors the system’s CFACTs compliance and acts as a liaison for Security issues with the ISSO
Capital Planning Analyst	<ul style="list-style-type: none"> • Work with the Program or Project Manager to update the Portfolio Management Tool to reflect the current status of the IT Investment. • Assists the P/PM in informing, updating, and completing required artifacts.
Governance Review Team	Performs the initial review of system characteristics for the production release.

Roles	Responsibilities
	<ul style="list-style-type: none"> • Monitors the GPR for consistency with the Production environment. • Determines if and when situational reviews are necessary for projects
Navigator	<p>Supports the Business Owner and Program Team in satisfying governance requirements and coordination with service centers, including OIT services, OAGM, and OFM Program Team</p> <ul style="list-style-type: none"> • Supports administrative functions including acquisition, budget, and investment reporting • Defines, designs, develops, tests, and implements IT solution. • Maintains Governance Profile Repository system characteristics
Program Team	<ul style="list-style-type: none"> • Supports administrative functions including acquisition, budget, and investment reporting • Defines, designs, develops, tests, and implements IT solution. • Maintains Governance Profile Repository system characteristics
TRB	Provide consultative services, as requested, to the programs to shape technology decisions to align with the CMS Technical Reference Architecture and Technology Roadmap
508 Clearance Coordinator	Verifies that the application complies with accessibility requirements

F. 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. 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.

More information can be found in [Appendix C - CPIC - Investment Management/Budget and Acquisition](#)

2. Information Security & Privacy

The CMS Authorization to Operate (ATO) must be in effect in order for a new system to go into operation.

The ATO must be maintained and all related security activities completed (e.g. annual Contingency Plan tabletop test, annual review of documentation, etc. for existing systems undergoing changes).

Security must be continually assessed with every production release. The project team must work with their ISSO and CRA to ensure that all CMS security procedures are followed at all times.

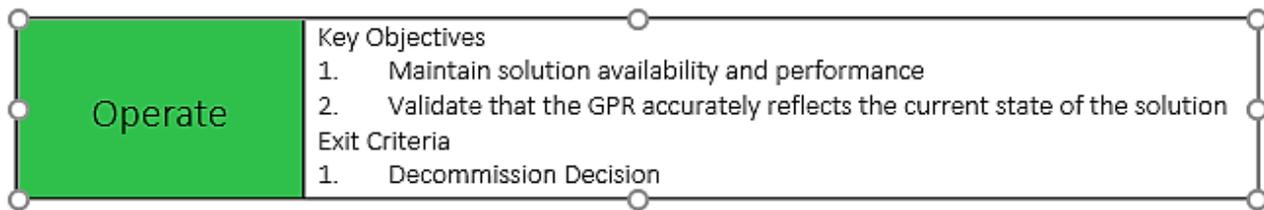
Accessibility - Section 508 testing must be completed and documented

3. Records management and retention schedule

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 can be found at their [website](#).

IV. Operate Phase



A. Overview

The Operate Phase is initiated immediately upon deployment of the solution to the Production environment. The Operate Phase includes Operations and Maintenance (O&M) 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. Steady operational status will be maintained, routine maintenance applied and sound security practices continued. 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).

The GPR must be reviewed and updated prior to every Production release when changes are needed. Business and program teams must maintain the currency and availability of their documentation to support internal reviews and audits from outside agencies. The inability to produce current documentation may impact 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 that all security standards are adhered to.

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	<ul style="list-style-type: none">● 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	<ul style="list-style-type: none">● Assists the P/PM to update the Portfolio Management Tool to reflect the current status of the IT Investment.● Assists the P/PM in informing of, updating, and completing, required artifacts.
Navigator	<ul style="list-style-type: none">● Maintains contact with the Business Owner to evaluate if technical solutions are satisfying current and emerging business needs
Program Team	<ul style="list-style-type: none">● 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.● Maintains the accuracy of solution characteristics in the GPR

E. Related Governance

1. Capital Planning and Investment Control (CPIC)

During this phase, the P/PM should be identifying lessons learned, identify emerging gaps in functionality, performance, or opportunities to improve the current state. OMB requires that these processes be documented by the P/PM and submitted to them upon request.

2. Information Security

The CMS ATO must be maintained and all related security activities completed (e.g. annual Contingency Plan tabletop test, annual review of documentation, etc.).

The Project Team is expected 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 can be found at their [website](#).

V. Retire Phase

Retire	CHECKLIST	Key Objectives
		Exit Criteria

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.

1. Business Owner Attestation

In the Retire Phase the operation of the system is discontinued. Extensive planning is done in order to define all the tasks that must be completed to decommission the system. Any remaining activities must be transitioned to a different process or system, contracts will be closed out, data needs to be archived according to the SORN or other guidelines, and hardware must be disposed of in accordance with Federal best practices. Most projects will simultaneously be in the O&M (Operations Phase) continuously working on current operations as well as decommissioning strategy and tasks (Retire Phase).

A. Information Requirements

Disposition Checklist

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

1. Data Center configuration items:

- User accounts, developer accounts, Firewall, security configurations, etc.
- Archive data, system documentation and software
- End/return software license agreements
- Close all CFACTS findings
- Submit Disposition Memo to the CISO
- Update the status with EA

B. Exit Criteria

1. Completed Disposition Checklist

C. Roles and Responsibilities

Role	Responsibilities
Business Owner	• Complete the disposition checklist
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

D. Related Governance

1. Information Security

Disposition section details within CFACTS must be completed, and the project closed and 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

VI. 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 will consist of a Technical Review Board (TRB) representative, EA, OAGM, OFM, and Security and Privacy representatives.

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 TLC policies
- To invoke situational reviews by the TRB or Governance Review Board, EA consults, and TechStat reviews when necessary and/or triggered by changes in the GPR

C. Technical Review Board (TRB) Consult

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 will also be leveraged for situational reviews as determined by the Governance Review Team.

D. TLC Resource Library

The TLC Resource Library is a hub to support businesses and programs in developing and delivering their IT solutions. The TLC Resource Library will host a variety of best practices, job aids, and templates to support lifecycle activities, and also access to support resources, such as TRB consults.

E. Enterprise Architecture (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 will also be leveraged for situational reviews as determined by the Governance Review Team.

VII. 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	Part of the Business Case, varying approaches to fulfilling the same business need are documented and compared 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
Authorization to Operate (ATO)	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

VIII. Appendix B – Monitored Fields

The Governance Profile Repository consists of key system characteristic values gathered from multiple sources including the annual CMS System Census performed by EA, CFACTS, and CPIC. Any changes to these fields will trigger a situational review.

This is a preliminary list of the data fields that will be monitored. More characteristics will be added.

Trigger Name	Trigger Fields	Potential Trigger Action(s)
Contingency Plan Review	Contingency Plan Expiration Date in CFACTS > current date	CFACTS Finding Entered
Contingency Plan Table Top Test	Contingency Plan test date in CFACTS is > 365 days	CFACTS Finding Entered
Security Assessment Done	Last Assessment Date in CFACTS > 365 days	CFACTS Finding Entered
System Security Plan Review	System Security Plan review date (available in CFACTS?) is > 365 days old	CFACTS Finding Entered
ATO Re-authorization Warning 1	Date Authorization Memo Expires in CFACTS = current date + 100 days	Ensure Re-authorization in progress
ATO Re-authorization Warning 2	Date Authorization Memo Expires in CFACTS = current date + 50 days	Ensure Re-authorization in progress
ATO Re-authorization Warning Final	Date Authorization Memo Expires in CFACTS = current date + 10 days	Ensure Re-authorization in progress
ATO Expiration	Date Authorization Memo Expires in CFACTS > current date	CFACTS Finding Entered, Risk based decision to shut down system until resolved
Business Program Alignment Change	CMS Business Function change in TLC GPR CMS Major Program Area change in TLC GPR Mission Essential Functions change in TLC GPR	EA Consult, TRB Review, Investment Review, TechStat
Data Type Change	Data Categories change in TLC GPR	EA Consult, TRB Review, Investment Review, TechStat
Section 508 Review	Section 508 Last Review Date in TLC GPR > current date - 6 months	508 Consult
Contract PoP End Warning 1	Contract Period End Date = current date + 60 Days	Ensure Renewal in progress
Contract PoP End Warning 2	Contract Period End Date = current date + 30 Days	Ensure Renewal in progress
Contract PoP End Warning Final	Contract Period End Date = current date + 5 Days	Ensure Renewal in progress
Major Architectural Changes	Fundamental Changes = Yes in TLC GPR	EA Consult, TRB Review, Investment Review, TechStat

Trigger Name	Trigger Fields	Potential Trigger Action(s)
Enterprise ELA Alignment	Software Product Name and Current Software Product Version does not equal Enterprise Name and Version for known ELA	TRB Review
Data Center Change	Data Center Name OR Data Center Address change in TLC GPR	EA Consult, TRB Review, Investment Review, TechStat
Funding Source(s) Change	FMIB # change in TLC GPR	Investment Review
New Software	Software Manufacturer OR Software Product Name are not currently used by CMS	TRB Research Spotlight, New EA Entry
Major Software Upgrade	Software Manufacturer AND Software Product Name is changed in TLC GPR OR Current Software Product Version significantly changes in TLC GPR	TRB Research Spotlight, TRB Review
TLC Compliance Warning 1	Reviews find TLC GPR not up to date or incorrect - 1st offense	Warning and 30 Days to Remediate
TLC Compliance Warning 2	Reviews find TLC GPR not up to date or incorrect- 2nd offense	TRB Review, CFACTs Finding Entered, OAGM Notification
TLC Compliance Warning 3+	Reviews find TLC GPR not up to date or incorrect - 3rd+ more	TRB Review, CFACTs Finding Entered, TechStat, ATO Revocation, OAGM STOP order

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

Investment Management/Budget & Acquisition

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 Capital Planning and Investment Control (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; (4) identify IT Investments that would result in shared benefits or costs for other Federal agencies or State or local governments; (5) provide for identifying quantifiable measurements for IT Investment net benefits and risks; and, (6) provide the means for senior management to obtain timely information regarding an Investment's progress.

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. One cannot exist without the other when IT projects are planned, developed, tested, and implemented correctly. 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 ensure someone from the CPIC Investment Management team is included within their 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 in order to better understand the purpose and functions.

The Select Phase, which coincides with the TLC Initiate phase, is considered the point at which the investment is justified. This is done 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 business case and alternatives analysis will be utilized by the GRB to determine if the project should be included in the CMS IT portfolio and thus funding requested for it. The acquisition strategy will be primarily utilized to determine if the overall approach to acquiring the assets needed to complete the project 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. This phase is considered the process of ensuring sound project management practices are being levied against selected investments and that the investments are on schedule, within budget, and meeting the scope of work. This is typically done through periodic reviews such as an operational analysis and post implementation review. OMB requires that these two processes be documented by the P/PM and submitted to them 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 post implementation reviews or PIRs are typically done within the 1st 6 months of project completion to identify lessons learned. The annual evaluations are utilized 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.

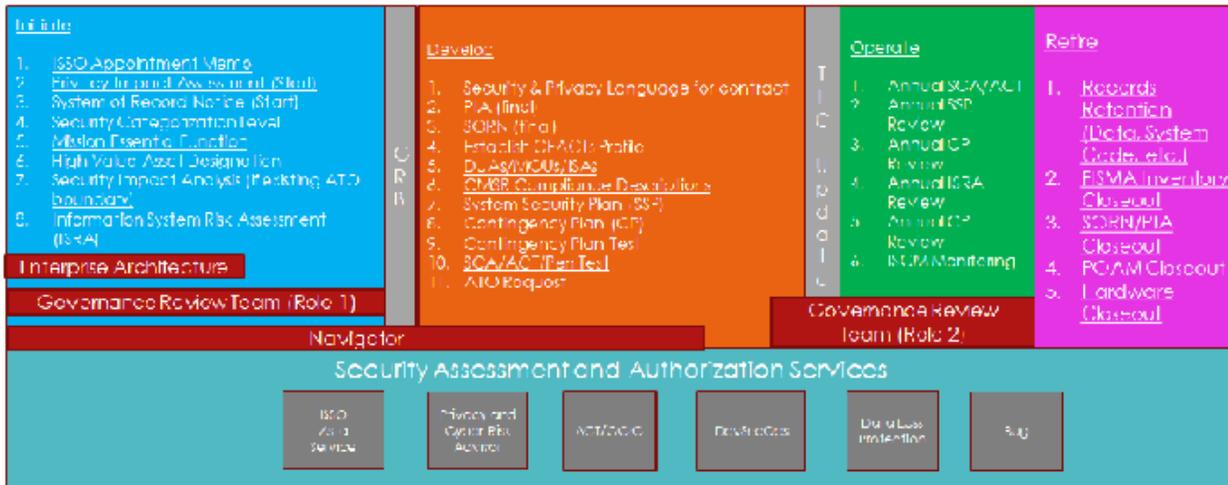
X. Appendix D – Security and Privacy

The Information Security & Privacy Group Advantage

Portfolio Program

[PLACEHOLDER]

TLC Security & Privacy Activities by Phase



Always Available Resources



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 Maintainer

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

DRAFT

XI. Appendix E - TLC Project Worksheet

TLC Project Worksheet

CMS Target Life Cycle Governance Review Board

Contains Business Case, Analysis of Alternatives, and GRB Decision

1. General Project Information

Project Name: *<Enter a name for the proposed project>*

Requested By: *<Enter Navigator or Business Component Representative Name>*

Business Owner: *<Enter Business Owner/Manager supporting this document>*

Contact Information: *<Enter email address and phone number of primary contact>*

Desired Start Date: *<Enter a desired start date for the requested project>*

Desired Go-Live Date: *<Enter a desired go-live date for the requested project>*

2. GRB Summary and Decision

Meeting Date/Time: *<Enter the time and date of the Board meeting>*

New System, Existing System, or Replacement?: *<Identify if this is a new system, existing system with enhancements, or replacement system>*

Board Decision: *<Approve or Disapprove>*

Board Recommendation

Based on the discussions on *<insert date>*, the Governance Review Board approves the following paths forward in order of preference:

1. *<Insert Preference #1>*
2. *<Insert Preference #2>*
3. *<Insert Preference #3>*
4.

<Describe any additional considerations, decisions, or risks from the Board regarding the implementation.>

The next step is for the Business Owner to select an approved solution alternative and notify the Governance Review Team (GRT) of their selection. The GRT will issue an investment life cycle ID number, which the business owner can use to request or allocate funding.

3. Project Description

3.1 Business Need

<Instructions: Provide a detailed explanation of the business need/issue/problem that the requested project will address, including any legislative mandates, regulations, etc. Include any expected benefits from the investment of organizational resources into the project. Please be sure to indicate clearly relevant deadlines (e.g., statutory deadlines that CMS must meet).>

Explain the benefits of developing an IT solution for this need.>

4. Alternatives and Analysis

<Instructions: The Alternatives and Analysis section should identify options and alternatives for the proposed project. Include a description of the approaches and an outline/description of each alternative considered. Include at least three viable alternatives: keeping things “as-is” or reuse existing people, equipment, or processes; and at least two additional alternatives. Identify your preferred solution.>

Some examples of alternatives to consider may include:

- *Buy vs. build vs. lease vs. reuse of existing system*
- *Commercial off the shelf (COTS) vs. Government off the shelf (GOTS)*
- *Mainframe vs. server-based vs. clustering vs. Cloud*

In your alternatives, include details such as:

- *Initial and ongoing costs*
- *Other financial considerations*
- *Security considerations*
- *Etc.>*

4.1 Alternative A

Summary: *<Provide a brief summary of the proposed IT solution including any associated software products, implementation approach (e.g. development/configuration, phases), costs (e.g. services, software, O&M), and potential acquisition approaches.>*

Acquisition Approach: *<Describe the approach to acquiring the products and services required to deliver the system, including potential contract vehicles.>*

Pros: *<Identify any aspects of this solution that positively differentiates this approach from other solutions.>*

Cons: *< Identify any aspects of this solution that negatively impact this approach.>*

Alternative A - Estimated Life Cycle Costs

TLC Phase	Current Year Estimated Cost	Current Year +1 Estimated Cost	Current Year +2 Estimated Cost	Current Year +3 Estimated Cost	Current Year +4 Estimated Cost	5-Year Estimated Costs
Initiate						\$0
Develop						\$0
Operate						\$0
TOTAL	\$0	\$0	\$0	\$0	\$0	\$0

Alternative A - Governance Review Board Assessment (circle one)

Preferred Acceptable Not Acceptable

4.2 Alternative B

Summary: <Provide a brief summary of the proposed IT solution including any associated software products, implementation approach (e.g. development/configuration, phases), costs (e.g. services, software, O&M), and potential acquisition approaches.>

Acquisition Approach: <Describe the approach to acquiring the products and services required to deliver the system, including potential contract vehicles.>

Pros: <Identify any aspects of this solution that positively differentiates this approach from other solutions.>

Cons: < Identify any aspects of this solution that negatively impact this approach.>

Alternative B - Estimated Life Cycle Costs

TLC Phase	Current Year Estimated Cost	Current Year +1 Estimated Cost	Current Year +2 Estimated Cost	Current Year +3 Estimated Cost	Current Year +4 Estimated Cost	5-Year Estimated Costs
Initiate						\$0
Develop						\$0
Operate						\$0
TOTAL	\$0	\$0	\$0	\$0	\$0	\$0

Alternative B - Governance Review Board Assessment (circle one)

Preferred Acceptable Not Acceptable

4.3 Alternative C

Summary: <Provide a brief summary of the proposed IT solution including any associated software products, implementation approach (e.g. development/configuration, phases), costs (e.g. services, software, O&M), and potential acquisition approaches.>

Acquisition Approach: <Describe the approach to acquiring the products and services required to deliver the system, including potential contract vehicles.>

Pros: <Identify any aspects of this solution that positively differentiates this approach from other solutions.>

Cons: < Identify any aspects of this solution that negatively impact this approach.>

Alternative C - Estimated Life Cycle Costs

TLC Phase	Current Year Estimated Cost	Current Year +1 Estimated Cost	Current Year +2 Estimated Cost	Current Year +3 Estimated Cost	Current Year +4 Estimated Cost	5-Year Estimated Costs
Initiate						\$0
Develop						\$0
Operate						\$0
TOTAL	\$0	\$0	\$0	\$0	\$0	\$0

Alternative C - Governance Review Board Assessment (circle one)

Preferred Acceptable Not Acceptable

4.4 Add additional alternatives if necessary>

5. Governance Review Team Recommendation

<This is only required if the Governance Review Team wishes to include an alternative which has not been discussed above, or comment on the proposed alternatives.>

6. Governance Review Board Meeting Participants

Role	Participants
Governance Review Board Members	<i><Identify all attending board members including Name (Component/Center/Office)></i>

Role	Participants
Business Owner and Navigator	<i><Identify the primary business owner and navigator including Name (Component/Center/Office). Additionally, identify the program/project manager for existing systems.></i>
Governance Review Team	<i><Identify the attending governance review team members including Name (Component/Center/Office)></i>
Subject Matter Experts	<i><Identify the attending subject matter experts including Name (Component/Center/Office)></i>
Other	<i><Identify additional board meeting attendees including Name (Component/Center/Office)></i>

DRAFT

XII. 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 lifecycle. 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. It is used in making a risk determination decision for the operation of the subject system. When the level of risk to the CMS enterprise is deemed acceptable, the system is granted 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 Enterprise Architecture enumeration of IT systems within CMS and relevant characteristics about them.
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	future

Acronym	Term	Definition
-	Disposition	Disposition is defined as retiring a capital asset once its useful life is completed or a replacement asset has superseded it. Disposition costs may be included in 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	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.
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 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	future
GPR	Governance Profile Repository	The preliminary list of GPR data elements are identified in Appendix B – Monitored Fields . Changes to these fields may indicate a change in the security or governance profile of a system.
GRB	Governance Review Board	future

Acronym	Term	Definition
-	Investment Lifecycle ID number	future
GRT	Governance Review Team	The GRT will consist of a Technical Review Board (TRB) representative, EA, OAGM, OFM, Security and Privacy representatives as the core members.
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).
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	future
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 are aimed at expanding the capacity of an asset or otherwise upgrading it to serve needs different from or significantly greater than those originally intended should be considered DME.
-	Material Change	A change to GPR profile 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	future
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).

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. The notice allows questions to be raised and resolved before the system is put into effect and ensures that privacy considerations have been addressed.
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 systems development lifecycle 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.
TRB	Technical Review Board	The CMS technical governance body for information technology (IT) projects that provides guidance to project teams on adhering to CMS technical standards and leveraging existing technologies (e.g., Shared Services).