Department of Health and Human Services

Centers for Medicare & Medicaid Services

CMS Expedited Life Cycle Process: Detailed Description

Version 3.4

August 14, 2015

Record of Changes

#	Date	Reference	A=Add M=Modify D=Delete	Description of Change	CR #
1	August 25, 2011	All	A	Initial Working Draft	NA
2	January 27, 2012	Complexity Focus Group	M	Section 2, Project Complexity Description	NA
3	March 05, 2012	Governance Team Review	A, M	• Section 1 edits for clarity, added Section 1.4 on starting a project • Section 2 and Section 6, removed references to Cost Estimation Tool (CET) • Section 5 alignment and consistency changes, consolidated artifacts definition, removed references to core and recommended artifacts. • Revised graphics for Figures 1-3, updated Figure 9 for consistency • Revised Section 6, Appendix, to align with Section 5 updates	NA
4	March 13, 2012	Governance Team Review	M	• Updated Figures 3, 6-13 • Updated Security Artifacts life cycle in Figure 9 and Sections 5 & 6	NA
5	March 14, 2012	CMS	M	• Changed Table/Figure captions and references to them. Added List of Tables in TOC.	NA
6	March 21, 2012	Governance Team Review	A, M	• Modified Figure 3 for CL 2 • Modified Section 6.2 to align with CL 2 • Figure 5 marked as sample. • Sections 1.3 and 2 minor updates • Section 4: added 4 roles, modified GO definition, deleted reference to ERR • Section 5 minor edits	NA
7	March 28, 2012	Governance Team Review	M	• Modified Figure 3 to correct IAT definition to Independent Assessment Team • Replaced Figure 5 with new Starting a Project graphic and revised accompanying text.	N/A
8	April 5, 2012	CMS	M	• Promoted Detailed Design Review to governance review for Complexity Level 3 • Removal of Project Startup Review	2012-01 2012-02
9	April 16, 2012	Governance Team Review	M	• Revised Figure 2: Expedited Life Cycle Process Flow, for improved 508 compliance, inclusion of the initial idea presentation	NA

#	Date	Reference	A=Add M=Modify D=Delete	Description of Change	CR #
10	May 3, 2012	Governance Team Review	M	• Revised Guidance Officer definition in Section 4	NA
11	May 16, 2012	Governance Team Review	M	• Revised Section 4, XLC Roles, to include Investment Owner	N/A
12	May 30, 2012	MITRE	A	• Editing and 508 compliance	N/A
13	August 10, 2012	CMS	M	• Removed incorrect references to federally owned systems in Section 5.	N/A
14	November 13, 2012	CMS	M	• Removed most references to Guidance Officer in anticipation of new OIS Business/Technology Liaison role	N/A
15	July 22, 2013	CMS	M	• Security changes to Table 4 and related sections.	12-007
16	December 20, 2013	CMS	M	• Changed XLC graphic • Updated Table 1 (Complexity) • Updated Table 4 (Artifacts)	13-002 13-008 12-007
17	August 27, 2014	CMS	M	1. Added references to Acquisition Strategy, per CR 14-002. 2. Corrected the following errors: • Removed the artifact "Disposition Closeout Certificate" from Table 4 and Section 5.5.3 on p. 38. This is not a valid artifact. • Corrected definition of "CIRT" (p. 7) • Removed all references to Guidance Officer (GO) • Added System Retirement Memo to Section 5.5.3.	14-002
18	November 13, 2014	CMS	M	Added Performance Test Plan and Results Template. Updated the definition of the Post Implementation Review (PIR).	14-006
19	November 21, 2014	CMS	M	Added to System Security Plan to Table 4. This item was overlooked in a prior release.	N/A
20	February 02, 2015	CMS	M	Updated CMS logo.	N/A
21	August, 14, 2015	CMS	M	Inserted updated swim lane diagram. Replaced Division of IT Governance with Division of Policy, Program Integration, & Governance	15-006
22	October 7, 2015	CMS	M	Replaced references to OIS with OEI OTS in Section 1.1 and replaced OIS with OEI in Section 1.4	N/A

Table of Contents

List of Figures

List of Tables

1. CMS Expedited Life Cycle Introduction

The Centers for Medicare & Medicaid Services (CMS) is committed to strengthening its systems development life cycle processes. Given the need to respond quickly to business demands, CMS created a streamlined model to guide and coordinate information technology (IT) projects, called the CMS Expedited Life Cycle (XLC).

The XLC offers a simplified, consistent IT oversight framework to assist:

- IT project managers
- Business owners
- Critical partners
- Other stakeholders

The XLC includes three project complexity levels to help teams identify which artifacts, reviews, and tests are needed for their projects. The primary purpose of these options is to balance speed and oversight appropriately with the complexity and risk associated with a particular IT project.

1.1 High-Level Process Overview

Six key activities bridge the project phases. Typically, once the idea has been defined, the project is reviewed for architectural compliance and IT investment. Once approved, the project team completes each life cycle phase with ongoing involvement from appropriate stakeholders. This includes involvement from the:

- Project team
- Governance boards
- Business owners
- CMS Office of Enterprise Information (OEI)
- CMS Office of Technology Solutions (OTS)
- Leadership

Figure 1 depicts the key, high-level activities associated with the development life cycle of a typical project. Each high-level activity has specific work associated with it and involves different stakeholders:

- **Activity 1: Staff Work**
  The project team defines the idea and creates the preliminary set of documentation, starting with the IT Intake Request Form. This documentation articulates the business need, scope, and high- level architecture.

- **Activity 2: Reviews**
  Activity 2 involves a Business Architecture and Technology Solutions (BATS) Board review to institutionalize governance of the shared services approach through initial needs assessments and architecture reviews. This constitutes the first XLC review, the Architecture Review (AR). The BATS Board may delegate the AR to the Technical Review Board (TRB).

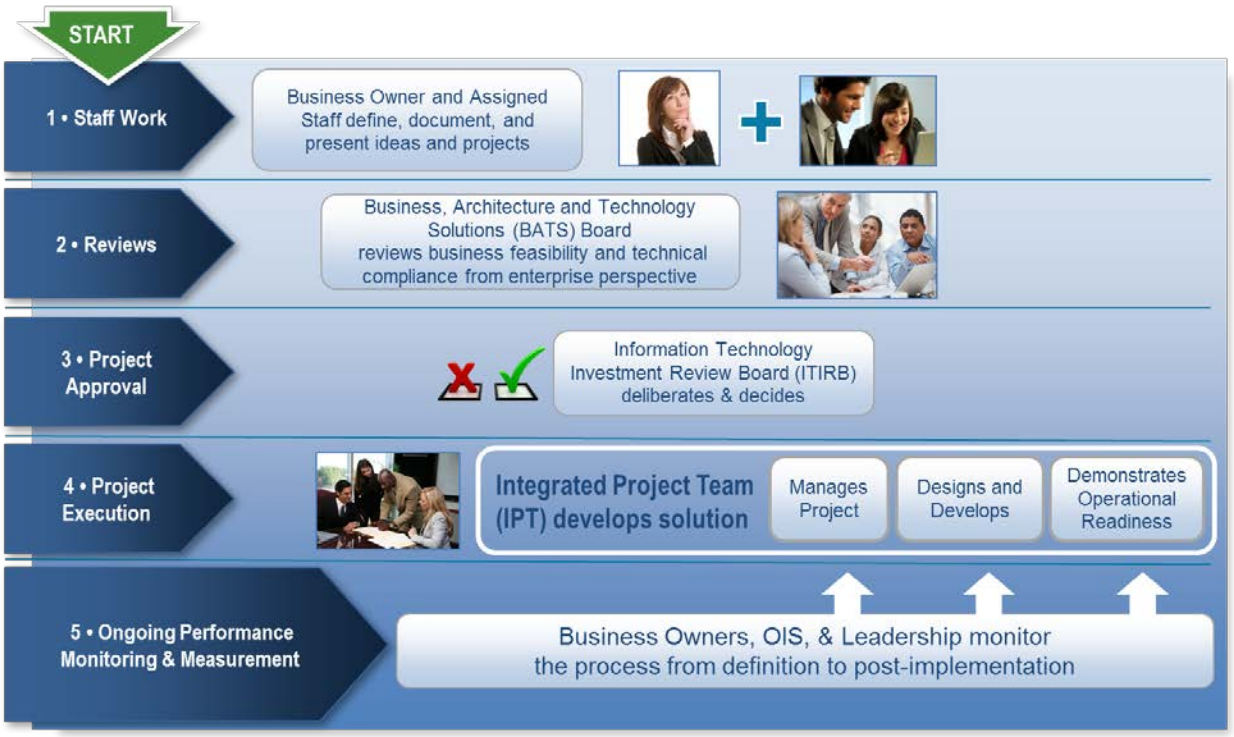


Figure 1. Five Key Activities

- **Activity 3: Project Approval**
  An approval from the BATS Board kicks off Activity 3, which culminates with an IT Investment Review Board (ITIRB) review that focuses on strategic, enterprise-level shared solutions. This constitutes the second XLC review, the Investment Selection Review (ISR).

- **Activity 4: Project Execution**
  The ITIRB approval marks the start of Activity 4, which constitutes the project execution and any reviews appropriate for that project, depending on the complexity level of that project.

- **Activity 5: Ongoing Performance Monitoring & Measurement**
  Activity 5 is the ongoing performance monitoring throughout the process.

1.2 Expedited Life Cycle Model

The XLC model provides a streamlined approach to project oversight and execution. It is the next generation of project life cycle processes with a flexible approach to project execution and governance, using a level of governance directly associated with each project's complexity. This model promotes agility, effective project review, and establishing appropriate oversight early in the process, increasing predictability and efficiency.

Figure 2 depicts the process flow of the five XLC key activities.

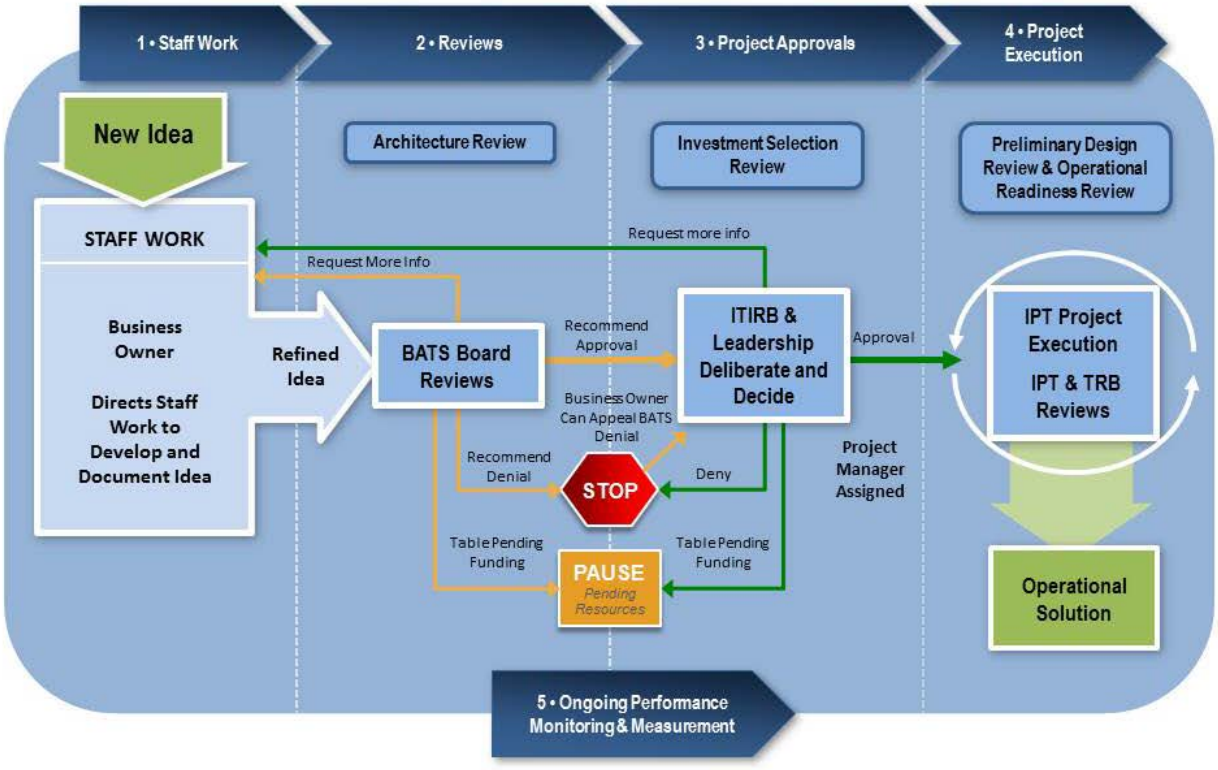


Figure 2: Expedited Life Cycle Process Flow

Figure 3. Expedited Life Cycle Model shows how the XLC provides three tailored options for projects to adopt, depending on the project's level of complexity.

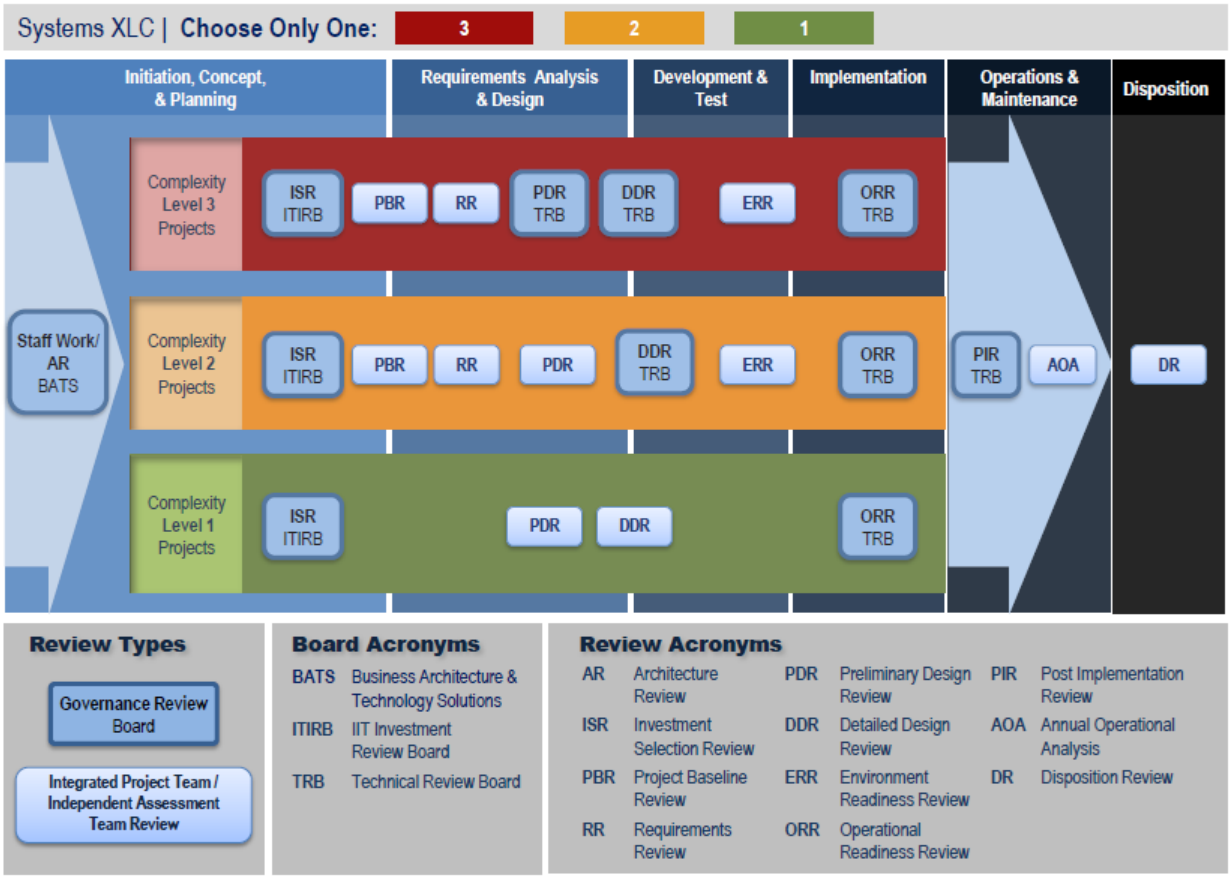


Figure 3. Expedited Life Cycle Model

Each complexity level includes two types of reviews:

- **Governance Board Reviews**: Scheduled with the appropriate CMS governance bodies and conducted with all relevant stakeholders. There are three or more governance board reviews, depending on the project's complexity level.
- **Integrated Project Team (IPT)/Independent Assessment Team (IAT) Reviews**: Conducted by the IPT/IAT with relevant stakeholders and guided by project complexity. The IPT may engage members of the governance boards for these reviews.

Each review provides the opportunity to assess project work to date, identify any potential issues, and ultimately approve the project to continue with the next phase of the life cycle. Each decision is based on a review of the artifacts associated with that particular review. Section 2 provides a high-level description of each tailored XLC option and associated review. Section 5 provides a detailed description of each XLC review and associated artifacts.

It is unlikely that any project will be required to produce every single artifact. **Table 4** outlines when the different artifacts should be started and completed. For artifacts spanning multiple phases, it is expected that updates to the preliminary artifact will be delivered and reviewed at the applicable reviews.

1.3 Project Process Agreement (PPA)

The PPA is a key XLC artifact that sets expectation and increases overall project predictability. It is a written agreement between the key stakeholders that establishes a common understanding of which reviews will be conducted for the project, which artifacts are appropriate, and which tests are necessary based on the project's complexity level as determined by the Project Manager/Business Owner.

Each PPA contains a complexity worksheet, a list of artifacts, a list of reviews, a list of tests, and a signature sheet. An Excel-based tool is used to create the PPA and as each tab is completed, the signature sheet is populated with the selected items from each list. The Division of Policy, Program Integration, & Governance (DPPIG) approves the PPA before it is baselined. DPPIG-assigned Project Consultants can approve a PPA, or a draft of the PPA can be sent to IT_Governance@CMS.hhs.gov for review and approval.

The approved PPA can be provided to a contractor as part of a request for proposal. As a proposal input, the PPA helps scope the expected work.

The PPA is a prediction based on the best knowledge available at the time. As a project's design and implementation details are discovered and refined, the project team may learn that the PPA needs to be updated. For example, a commercial off-the-shelf (COTS) product may not perform as expected and unforeseen development may be required. This unanticipated development may change a project's complexity level and, as a result, may require that the number and type of reviews, associated artifacts, and tests have to be updated.

Sometimes these changes are identified at an early Governance review. Whenever such changes are identified, the PPA should be updated to reflect the implications of a more complete understanding of the solution. Changing the PPA baseline ensures that cost, schedule, technical, and risk baselines are synchronously updated. Updated signatures show that the key stakeholders understand the implications of this new information and that they agree with the revised and newly baselined plan.

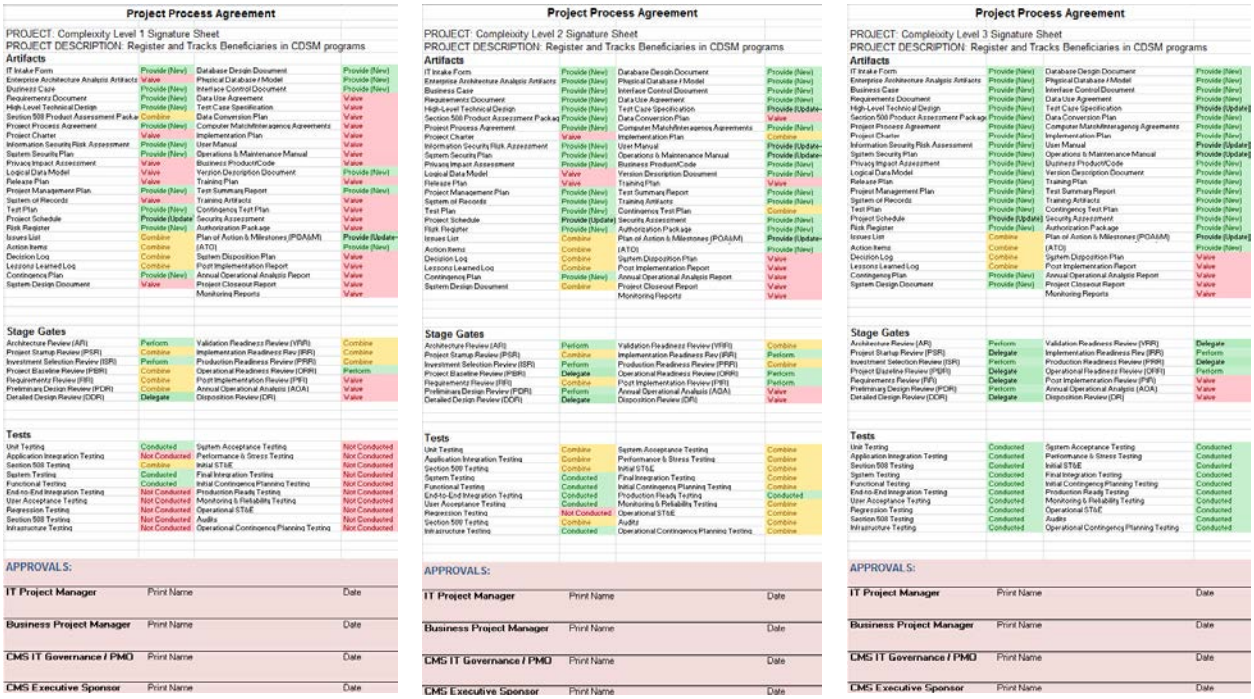
The Excel-based PPA uses color codes to provide a visual summary of expected work.

Color Codes:

- For each project, relevant artifacts, reviews, and tests to be performed are highlighted in green.
- When the decision is made for a project to combine artifacts, reviews, or tests, these items are highlighted in yellow.
- Items that are waived for a project because they are not applicable to a solution are highlighted in pink.

Figure 4 shows samples of Complexity Level 1, 2, and 3 signature sheets. Comparing the samples shows how stakeholders could agree upon relevant artifacts, reviews, and tests based on the chosen XLC option. Section 2 describes these options and complexity levels in detail.

Complexity Level 1 **Complexity Level 2** **Complexity Level 3**



Project Process Agreement

PROJECT: Complexity Level 1 Signature Sheet
PROJECT DESCRIPTION: Register and Tracks Beneficiaries in CDSM programs

Artifacts

IT Intake Form	Provide (New)	Database Design Document	Provide (New)
Enterprise Architecture Analysis Artifacts	Waive	Physical Database / Model	Provide (New)
Business Case	Provide (New)	Interface Control Document	Provide (New)
Requirements Document	Provide (New)	Data Use Agreement	Waive
High-Level Technical Design	Provide (New)	Test Case Specification	Waive
Section 508 Product Assessment Package	Combine	Data Conversion Plan	Waive
Project Process Agreement	Provide (New)	Computer Matching Agreements	Waive
Project Charter	Waive	Implementation Plan	Waive
Information Security Risk Assessment	Provide (New)	User Manual	Waive
System Security Plan	Provide (New)	Operations & Maintenance Manual	Waive
Privacy Impact Assessment	Waive	Business Product/Code	Waive
Logical Data Model	Waive	Version Description Document	Provide (New)
Release Plan	Waive	Training Plan	Waive
Project Management Plan	Provide (New)	Test Summary Report	Provide (New)
System of Records	Waive	Training Artifacts	Waive
Test Plan	Provide (New)	Contingency Test Plan	Waive
Project Schedule	Provide (Update)	Security Assessment	Waive
Risk Register	Provide (New)	Authorization Package	Waive
Issues List	Combine	Plan of Action & Milestones (POA&M)	Provide (Update)
Action Items	Combine	(ATO)	Provide (New)
Decision Log	Combine	System Disposition Plan	Waive
Lessons Learned Log	Combine	Post Implementation Report	Waive
Contingency Plan	Provide (New)	Annual Operational Analysis Report	Waive
System Design Document	Waive	Project Closeout Report	Waive
		Monitoring Reports	Waive

Stage Gates

Architecture Review (ARI)	Perform	Validation Readiness Review (VRR)	Combine
Project Startup Review (PSR)	Combine	Implementation Readiness Rev (IRR)	Combine
Investment Selection Review (ISR)	Perform	Production Readiness Review (PRR)	Combine
Project Baseline Review (PBR)	Combine	Operational Readiness Review (ORR)	Perform
Requirements Review (RR)	Combine	Post Implementation Review (PIR)	Waive
Preliminary Design Review (PDR)	Combine	Annual Operational Analysis (AOA)	Waive
Detailed Design Review (DDR)	Delegate	Disposition Review (DR)	Waive

Tests

Unit Testing	Conducted	System Acceptance Testing	Not Conducted
Application Integration Testing	Not Conducted	Performance & Stress Testing	Not Conducted
Section 508 Testing	Combine	Initial ST&E	Not Conducted
System Testing	Conducted	Final Integration Testing	Not Conducted
Functional Testing	Conducted	Initial Contingency Planning Testing	Not Conducted
End-to-End Integration Testing	Not Conducted	Production Ready Testing	Not Conducted
User Acceptance Testing	Not Conducted	Monitoring & Reliability Testing	Not Conducted
Regression Testing	Not Conducted	Operational ST&E	Not Conducted
Section 508 Testing	Not Conducted	Audits	Not Conducted
Infrastructure Testing	Not Conducted	Operational Contingency Planning Testing	Not Conducted

APPROVALS:

IT Project Manager	Print Name	Date
Business Project Manager	Print Name	Date
CMS IT Governance / PMO	Print Name	Date
CMS Executive Sponsor	Print Name	Date

Project Process Agreement

PROJECT: Complexity Level 2 Signature Sheet
PROJECT DESCRIPTION: Register and Tracks Beneficiaries in CDSM programs

Artifacts

IT Intake Form	Provide (New)	Database Design Document	Provide (New)
Enterprise Architecture Analysis Artifacts	Provide (New)	Physical Database / Model	Provide (New)
Business Case	Provide (New)	Interface Control Document	Provide (New)
Requirements Document	Provide (New)	Data Use Agreement	Provide (New)
High-Level Technical Design	Provide (New)	Test Case Specification	Provide (Update)
Section 508 Product Assessment Package	Provide (New)	Data Conversion Plan	Waive
Project Process Agreement	Provide (New)	Computer Matching Agreements	Provide (New)
Project Charter	Waive	Implementation Plan	Combine
Information Security Risk Assessment	Provide (New)	User Manual	Provide (Update)
System Security Plan	Provide (New)	Operations & Maintenance Manual	Provide (Update)
Privacy Impact Assessment	Provide (New)	Business Product/Code	Provide (New)
Logical Data Model	Waive	Version Description Document	Provide (New)
Release Plan	Waive	Training Plan	Waive
Project Management Plan	Provide (New)	Test Summary Report	Provide (New)
System of Records	Provide (New)	Training Artifacts	Provide (New)
Test Plan	Provide (New)	Contingency Test Plan	Combine
Project Schedule	Provide (Update)	Security Assessment	Provide (New)
Risk Register	Provide (New)	Authorization Package	Provide (New)
Issues List	Combine	Plan of Action & Milestones (POA&M)	Provide (Update)
Action Items	Combine	(ATO)	Provide (New)
Decision Log	Combine	System Disposition Plan	Waive
Lessons Learned Log	Combine	Post Implementation Report	Waive
Contingency Plan	Provide (New)	Annual Operational Analysis Report	Waive
System Design Document	Combine	Project Closeout Report	Waive
		Monitoring Reports	Waive

Stage Gates

Architecture Review (ARI)	Perform	Validation Readiness Review (VRR)	Combine
Project Startup Review (PSR)	Combine	Implementation Readiness Rev (IRR)	Perform
Investment Selection Review (ISR)	Perform	Production Readiness Review (PRR)	Combine
Project Baseline Review (PBR)	Delegate	Operational Readiness Review (ORR)	Perform
Requirements Review (RR)	Combine	Post Implementation Review (PIR)	Perform
Preliminary Design Review (PDR)	Perform	Annual Operational Analysis (AOA)	Waive
Detailed Design Review (DDR)	Delegate	Disposition Review (DR)	Waive

Tests

Unit Testing	Combine	System Acceptance Testing	Combine
Application Integration Testing	Combine	Performance & Stress Testing	Combine
Section 508 Testing	Combine	Initial ST&E	Combine
System Testing	Conducted	Final Integration Testing	Combine
Functional Testing	Conducted	Initial Contingency Planning Testing	Combine
End-to-End Integration Testing	Conducted	Production Ready Testing	Conducted
User Acceptance Testing	Conducted	Monitoring & Reliability Testing	Combine
Regression Testing	Not Conducted	Operational ST&E	Combine
Section 508 Testing	Combine	Audits	Combine
Infrastructure Testing	Conducted	Operational Contingency Planning Testing	Combine

APPROVALS:

IT Project Manager	Print Name	Date
Business Project Manager	Print Name	Date
CMS IT Governance / PMO	Print Name	Date
CMS Executive Sponsor	Print Name	Date

Project Process Agreement

PROJECT: Complexity Level 3 Signature Sheet
PROJECT DESCRIPTION: Register and Tracks Beneficiaries in CDSM programs

Artifacts

IT Intake Form	Provide (New)	Database Design Document	Provide (New)
Enterprise Architecture Analysis Artifacts	Provide (New)	Physical Database / Model	Provide (New)
Business Case	Provide (New)	Interface Control Document	Provide (New)
Requirements Document	Provide (New)	Data Use Agreement	Provide (New)
High-Level Technical Design	Provide (New)	Test Case Specification	Provide (Update)
Section 508 Product Assessment Package	Provide (New)	Data Conversion Plan	Provide (New)
Project Process Agreement	Provide (New)	Computer Matching Agreements	Provide (New)
Project Charter	Provide (New)	Implementation Plan	Provide (New)
Information Security Risk Assessment	Provide (New)	User Manual	Provide (Update)
System Security Plan	Provide (New)	Operations & Maintenance Manual	Provide (Update)
Privacy Impact Assessment	Provide (New)	Business Product/Code	Provide (New)
Logical Data Model	Provide (New)	Version Description Document	Provide (New)
Release Plan	Provide (New)	Training Plan	Provide (New)
Project Management Plan	Provide (New)	Test Summary Report	Provide (New)
System of Records	Provide (New)	Training Artifacts	Provide (New)
Test Plan	Provide (New)	Contingency Test Plan	Provide (New)
Project Schedule	Provide (Update)	Security Assessment	Provide (New)
Risk Register	Provide (New)	Authorization Package	Provide (New)
Issues List	Combine	Plan of Action & Milestones (POA&M)	Provide (Update)
Action Items	Combine	(ATO)	Provide (New)
Decision Log	Combine	System Disposition Plan	Waive
Lessons Learned Log	Combine	Post Implementation Report	Waive
Contingency Plan	Provide (New)	Annual Operational Analysis Report	Waive
System Design Document	Provide (New)	Project Closeout Report	Waive
		Monitoring Reports	Waive

Stage Gates

Architecture Review (ARI)	Perform	Validation Readiness Review (VRR)	Delegate
Project Startup Review (PSR)	Delegate	Implementation Readiness Rev (IRR)	Perform
Investment Selection Review (ISR)	Perform	Production Readiness Review (PRR)	Delegate
Project Baseline Review (PBR)	Delegate	Operational Readiness Review (ORR)	Perform
Requirements Review (RR)	Delegate	Post Implementation Review (PIR)	Waive
Preliminary Design Review (PDR)	Perform	Annual Operational Analysis (AOA)	Waive
Detailed Design Review (DDR)	Delegate	Disposition Review (DR)	Waive

Tests

Unit Testing	Conducted	System Acceptance Testing	Conducted
Application Integration Testing	Conducted	Performance & Stress Testing	Conducted
Section 508 Testing	Conducted	Initial ST&E	Conducted
System Testing	Conducted	Final Integration Testing	Conducted
Functional Testing	Conducted	Initial Contingency Planning Testing	Conducted
End-to-End Integration Testing	Conducted	Production Ready Testing	Conducted
User Acceptance Testing	Conducted	Monitoring & Reliability Testing	Conducted
Regression Testing	Conducted	Operational ST&E	Conducted
Section 508 Testing	Conducted	Audits	Conducted
Infrastructure Testing	Conducted	Operational Contingency Planning Testing	Conducted

APPROVALS:

IT Project Manager	Print Name	Date
Business Project Manager	Print Name	Date
CMS IT Governance / PMO	Print Name	Date
CMS Executive Sponsor	Print Name	Date

Figure 4. Complexity Level 1, 2, and 3 Project Process Agreement Samples

1.4 Starting an XLC Project

Figure 5 shows the three-step process for getting an IT project started.

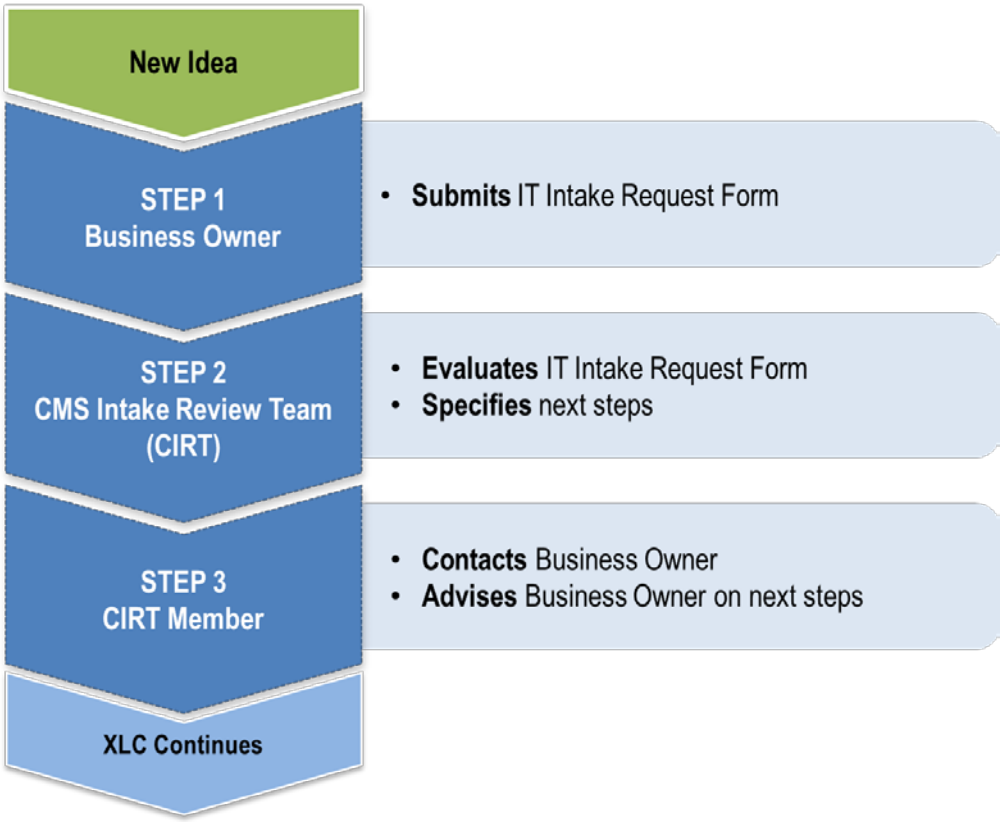


Figure 5. Starting an XLC Project

- **Step 1:** Starting a project begins with an idea. If the idea is likely to involve information technology, then the Business Owner (BO) drafts and submits an IT Intake Request Form. This form can be a preliminary form and notifies OEI that a Business Owner may need some help.

- **Step 2:** The CMS Intake Review Team (CIRT) evaluates the IT Intake Request Form. The CIRT specifies next steps and recommends assignment of a CIRT member to help the Business Owner navigate the startup process.

- **Step 3:** The assigned CIRT member contacts and works with the BO to initiate the project. Tasks performed at this stage may include assessing project complexity and risk, developing the Project Process Agreement, and developing Enterprise Architecture analysis artifacts as needed.

2. System Development XLC Options

The XLC provides business owners and IT project managers three tailored XLC oversight levels to manage a project. Each project evaluates the risks of the development effort and assesses its project complexity. Determining complexity level guides a project in the identification of:

1. Reviews needed and those that may be combined or waived
2. Artifacts needed and those that may be updated, combined or waived
3. Tests needed and those that may be combined or not conducted

These results help you understand the scope of work required for a project and support the development of a project plan, including schedule and rough order of magnitude (ROM) costs.

Determining complexity requires some insight into the systems development process. As a project starts, the CIRT assesses the project's experience with the XLC. As needed, the CIRT identifies resources to provide advice and process guidance.

2.1 Project Complexity Categories

CMS defined three Project Complexity Levels with the following characteristics:

2.1.1 Complexity Level 3 Projects

A Complexity Level 3 project is defined as either of the following:

- A project that requires a new, one-of-a-kind design and development effort to support an enterprise, center, or department-specific IT solution
- A project for a system that has or will have significant security and risk implications.

This could be an initial, major development, modernization, or enhancement effort and requires project teams to document detailed requirements, design, and technical solution specifications. Examples include:

- Implementing COTS software and/or hardware and integrating within existing systems/ environment
- Developing new code on a new or existing system
- Creating a new shared service.

Due to the unique challenges in delivering a Complexity Level 3 solution, more stage gate reviews or checkpoints are needed to ensure that these projects remain on track.

2.1.2 Complexity Level 2 Projects

A Complexity Level 2 project is defined as either of the following:

- A project that requires an isolated change with minimal impact to existing systems/ environments and does not significantly affect the state of any security controls or requirements

- A project that requires minor changes to one or more systems/environments that are incremental to the initial build, with limited impact, and do not significantly affect the state of any security controls or requirements.

Examples include:

- Implementing COTS software and/or hardware with no integration required
- Making minor changes to hardware capacity, adding storage, etc.

There is less risk and, in some ways, less work required to deliver a Complexity Level 2 solution, although some oversight is still warranted at key decision points. Several stage gate reviews or checkpoints are needed, but not as many as are needed to manage a Complexity Level 3 effort.

2.1.3 Complexity Level 1 Project

A Complexity Level 1 project is defined as a project that requires minor changes to existing services, systems, and/or environments and does not affect the state of any security controls or requirements. Examples include:

- Using existing shared services
- Implementing incremental data and configuration changes (providing that information is not repurposed and no security related configuration parameters are affected).

The least risky solutions usually involve repackaging proven capability in straightforward, proven ways. For Complexity Level 1 projects, since existing components have already navigated the XLC, relatively few stage gate reviews or checkpoints are needed to keep the project on track. **Note:** Using existing components that are approved for a lower security level than that required for the system is not permitted.

2.2 Completing the Goals of the Project Complexity Assessment

Completing a project complexity analysis leverages expertise from both the project manager/business owner and the Division of Policy, Program Integration, & Governance. It facilitates early planning by right-sizing the life cycle to meet the project's unique needs. This ensures sufficient reviews to manage known risk and identifies needed artifacts to communicate design and development decisions among stakeholders. The process encourages reuse of existing shared services because they are less risky, less costly, and less time-consuming to implement. Using consistent complexity analysis allows improvements to the process, enabling future projects to benefit from applying lessons learned.

Table 1 describes the criteria used for rating project characteristics in the evaluation to determine project complexity. Each project characteristic is assigned a complexity rating based on the Rating Guidance.

Working with the IPT, the project manager/business owner ensures that the specified stage gate reviews for the project's complexity swim-lane are performed, as shown in **Figure 3**. The project manager/business owner may add any reviews to this minimum set that are deemed necessary to manage risk to the project's success. This includes any project-unique reviews as well. Section 3 describes the risks of not performing a particular stage gate review.

The project manager/business owner , can identify the needed artifacts using the Excel-based PPA. The PPA describes each artifact, and these descriptions, used in conjunction with the project characteristic complexity determination from above, enable the business owner to make an informed decision about the need for an artifact. For example, if the project involves high data complexity, it will probably need a logical data model, a database design document, a physical data model, as well as appropriate test plans and test cases.

Table 1. Table for Rating Project Characteristics to Determine Overall Project Complexity

Project Characteristic	Complexity Level	Rating Guidance	Your Project's Level?
Shared Services Implications	3	Creating new shared service(s)	**1, 2, or 3 (select one)**
	2	Modifying existing shared service(s)	
	1	Using existing shared service(s) as is	
Program / Business Process Profile *with Design / Development Implications*	3	New business process model, or process that may lead to significant cross program coordination and/or significant coordination with external business partners and/or developing new code on a new or existing system	**1, 2, or 3 (select one)**
	2	Some new requirements and information flows, minor changes to code in an existing system	
	1	Requirements and information flows are similar to current programs, no new code	
Privacy Implications	3	New system, service or environment with any Personally Identifiable Information (PII), Personal health Information (PHI), or Federal Taxpayer Information (FTI) data that is used, accessed, stored, or transmitted **OR** Changes to a system, service or environment that has implications to PII, PHI, or FTI data that is used, accessed, stored, or transmitted	**1, 2, or 3 (select one)**
	2	N/A – Privacy is either Complexity Level 1 or 3	
	1	No PII, PHI, or FTI data **OR** Changes to a system, service or environment that has no implications to PII, PHI, or FTI data that is used, accessed, stored, or transmitted	

Project Characteristic	Complexity Level	Rating Guidance	Your Project's Level?
Security Category	3	New system, service or environment with any: • Investigation, intelligence-related, and security information • Mission-critical information **OR** Changes to existing service, system or environment that affects the state of any: • Investigation, intelligence-related, and security information • Mission-critical information	**1, 2, or 3 (select one)**
	2	New system, service or environment with any: • Information about persons • Financial, budgetary, commercial, proprietary or trade secret information • Internal administration • Other Federal agency information • New technology or controlled scientific information • Operational information • System configuration management information **OR** Changes to existing service, system or environment that affects the state of any: • Information about persons • Financial, budgetary, commercial, proprietary or trade secret information • Internal administration • Other Federal agency information • New technology or controlled scientific information • Operational information • System configuration management information	
	1	New system, service or environment with any: • Other sensitive information • Public information **OR** Changes to existing service, system or environment that affects the state of any: • Other sensitive information • Public information **OR** No implications to any security controls	

Project Characteristic	Complexity Level	Rating Guidance	Your Project's Level?
Data Complexity *ties to data's financial implications*	3	• Completely new data for the agency • Data serves as a corporate asset	**1, 2, or 3 (select one)**
	2	• Some new data is introduced	
	1	• Data is similar to existing agency systems • Data scope focused on one service/system/domain	
Interface Complexity	3	New interface or change(s) to an existing interface that involves: • Interaction with non-federal agencies in business rules • Data access via Internet • Extensive interaction with other systems, especially external organizations and agencies • Shared service or system access via Internet • Extensive interactions with other systems, databases, or new/updated COTS products	**1, 2, or 3 (select one)**
	2	New interface or change(s) to an existing interface that involves: • Interaction with other federal agencies in business rules • Data access via extranet • Moderate interaction with other systems, especially external organizations and agencies • Shared service or system access via extranet • Moderate interaction with other systems, databases, or new/updated COTS products	
	1	New interface or change(s) to an existing interface that involves: • No interaction w/ external organization in business rules • Data access via internal Department of Health and Human Services (HHS) network access only • No interaction with other systems, especially external organizations and agencies • Shared service or system access via internal HHS network access only • No interaction with other systems, databases, or new/updated COTS products **OR** • No changes to any interface	

Once **Table 1** is completed, the appropriate complexity level can be determined using the decision tree shown in **Table 2**. The second tab of the PPA combines these tables into one worksheet.

ROM cost can be determined by preparing a Basis of Estimate (BOE). The BOE should be based on comparison of the proposed project to other similar, completed projects. The BOE would note similarities and differences between completed projects and the proposed project and include appropriate adjustments to the costs for those completed projects. The Division of IT Investment Management provides a Cost Estimation Tool that offers a more rigorous cost estimation capability.

Table 2. Decision Tree for Overall Project Complexity Determination

	Results from the Project Characteristic Complexity Rating Worksheet (Figure 6)		**Project Complexity Level**
	More than one Complexity Level 3 project characteristic	**… then your project is complexity level:**	**3**
If your project has…	Only one Complexity Level 3 project characteristic -or- No Complexity Level 3 project characteristics and more than one Complexity Level 2 project characteristic		**2**
	No Complexity Level 3 project characteristics and only one Complexity Level 2 project characteristic -or- All Complexity Level 1 project characteristics		**1**

3. XLC Risk Considerations

When planning project activities and life cycle processes, it is important to consider the risk of waiving a review and plan appropriate mitigation strategies to ensure project success. **Table 3** describes the potential risks of waiving individual reviews. Please note: Any portion of a review designated as a Security Gate cannot be waived.[1]

Table 3. Risk of Waiving a Review

Review	Risk of Waiving Review
Architecture Review (AR)	• Causes high-level technical design to begin with incomplete understanding of desired solution and relationships to existing systems. • Redundancy risk, missed leverage opportunity, and potential conflicts with CMS IT strategy.
Investment Selection Review (ISR)	• Project is added to CMS investment portfolio and funds are committed without an assessment of soundness, viability, and worthiness.
Project Baseline Review (PBR)	• Work begins without a baseline plan, complicating the ability to provide direction and track progress against integrated cost, schedule, and technical baselines.
Requirements Review (RR)	• Design begins without requirement reconciliation with business needs. • Any unexpected issues that drive cost and schedule variances are likely to become more exaggerated later.
Preliminary Design Review (PDR)	• Detailed design begins without high-level application architectural review to validate software and external interfaces or verification that design satisfies requirements. • Any unexpected high-level design issues that drive cost and schedule variances are likely to drive further variances later in the life cycle.
Detailed Design Review (DDR)	• Development begins without assurance that design meets stated business needs. Solutions developed from incomplete or unworkable design are likely to have performance gaps, costing time and money to fix. • Any unexpected detailed design issues that drive cost and schedule variances are likely to drive further variances in development, integration, and verification.
Environment Readiness Review (ERR) 1: Validation Readiness Review (VRR)	• System/application testing commences without a formal handoff from development to test. Causes a lack of controlled baseline, clear statement of functionality status, formal turnover of any required work-around, or initiation of formal configuration management procedures. • Leads to an uncontrolled baseline with errors and fixes. • Any unexpected development issues that drive cost and schedule variances often drive further variances in integration and verification.

[1] Refer to *RMH Volume I Chapter 1, Risk Management in the XLC*. This document is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

Review	Risk of Waiving Review
ERR 2: Implementation Readiness Review (IRR)	• The system/application will move to an implementation (production-like) environment without a formal handoff from configuration management to implementation or rules for communication. The handoff usually includes verification that it meets requirements, statement of what function is and is not working, and formal turnover of any required work-around. • Any unexpected integration and verification issues that drive cost and schedule variances may drive further variances in the next levels of testing.
ERR 3: Production Readiness Review (PRR)	• The system/application moves to the production environment without a formal handoff from implementation or rules for communication. Handoff usually includes verification that it meets performance requirements, statement of what function is and is not working, formal turnover of any required work-around, and reconciliation with operations and maintenance procedures. • Any unexpected integration and verification issues that drive cost and schedule variances may drive further variances in later testing as well as production.
Operational Readiness Review (ORR)	• The system/application is put into production without verification that it meets performance requirements and that operation and maintenance procedures ensure prompt system recovery without loss of data.

4. XLC Roles

Given the risks associated with waiving a review, the XLC recommends the use of the Integrated Project Team (IPT) and/or an Independent Assessment Team (IAT) for delegated reviews. The XLC also recommends using the Technical Review Board (TRB) for consultations. When using contractors or third parties, the XLC recommends considering vender certifications (at least Capability Maturity Model Integration Level 3, ISO 9000) before delegating any production of artifacts or other aspects of the CMS XLC process.

Role of Business Architecture and Technology Solutions (BATS) Board

The Business Architecture and Technology Solutions (BATS) Board conducts the Architecture Review. The BATS Board may conduct ISRs when delegated by the ITIRB. The BATS Board may delegate the Architecture Review to the TRB.

Role of Business Owner (BO)

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.

Role of CMS Intake Review Team (CIRT)

The CMS Intake Review Team (CIRT) initially assesses the IT Intake Form. It ensures known architecture issues (analysis, integration, logical/physical models, and current and future state analysis) are addressed in the staff work leading to an Architecture Review. The CIRT also provides transition guidance related to business, data, applications, and technology to ensure appropriate strategic and tactical issues are considered when formulating an IT project.

Role of Contractors / Third Parties

For reviews, contractors/third parties may be used for developing review artifacts and other required materials. The XLC recommends using certified vendors with at least Capability Maturity Model Integration Level 3 assessment and ISO 9000 certification. Other CMS certification may be relevant depending on the project and content.

Role of Division of Policy, Program Integration, & Governance (DPPIG)

The Division of Policy, Program Integration, & Governance (DPPIG) is the CMS organizational unit responsible for IT governance. PPIG facilitates the intake of IT project requests, advises business owners and technical staff on navigating the XLC, and approves Project Process Agreements.

Role of Environment Owner

The Environment Owner provides development, validation, implementation and production environments for new applications prior to implementation in the data center.

Role of Executive Steering Committee (ESC)

The Executive Steering Committee (ESC) serves as management authority, providing senior management leadership for the successful and timely completion of IT projects to meet the business needs. The ESC provides management oversight and guidance to the Business Owner and/or Contracting Officer's Representative (COR) and makes final decisions on the priority, risk, and potential impact of changes to the project objectives, operations, quality, schedule, performance, budget, and other resources related to the IT project. The ESC monitors the progress and status of the IT projects and, if necessary, adjusts both project and business needs and priorities to ensure success of the IT projects and Agency mission.

Role of Independent Assessment Team (IAT)

An Independent Assessment Team (IAT) is a group of experienced and skilled practitioners who are free of biases, conflicts of interests, and political influences. An IAT team's responsibilities could include conducting delegated reviews. IATs keep the project team and stakeholders informed of the project's true status by assessing the maturity of business and technical processes; determining requirements adherence, changes, and impacts; evaluating technology and other risks; and measuring progress towards cost, schedule, and performance goals. The XLC recommends using an IAT for delegated reviews to ensure an outside and expert perspective in lieu of governance reviews.

Role of Information Technology Investment Review Board (ITIRB)

The IT Investment Review Board (ITIRB) is the executive review and decision-making body for CMS IT investment management. It reviews and approves IT initiatives and expenditures. In the XLC, the primary role of the ITIRB is to conduct the Investment Selection Review.

Role of Integrated Project Team (IPT)

The Integrated Project Team (IPTs) is a cross-functional or multidisciplinary group of individuals that is organized and collectively responsible for the specific purpose of delivering a product to an internal or external customer. IPTs are typically chaired by the Program or Project Manager and may include an IT project manager and a business project manager. The XLC recommends that the IPT provide a full range of IT support, covering requirements, design, development, data, infrastructure, testing, operations, and system integration if needed. Critical Partners (Subject Matter Experts) and business owner representatives assist the Project Manager with planning and executing the project and may also participate in delegated life cycle reviews such as the Project Baseline Review (PBR). These experts include representatives from Enterprise Architecture (EA) and Capital Planning and Investment Control (CPIC) as well as specialists in budget, acquisition, systems engineering, business ownership, security, Section 508, and privacy.

Role of the Investment Manager

In the XLC an Investment Manager (IM) leads the preparation for an Annual Operational Assessment (AOA) that examines the performance of a portfolio of projects. The IM coordinates various Business Owners' participation as appropriate for the AOA and is responsible for planning and executing the investment to achieve approved baselines. The IM may or may not be a subject matter expert in the business area supported by the investment.

Role of the Project Consultant

The main responsibility of the Project Consultant is to assist Business Owners in navigating the XLC.

Role of Technical Review Board (TRB)

The Technical Review Board (TRB) is involved in the XLC governance reviews. If scheduling a particular TRB review may cause a delay, the project may choose to continue progress pending feedback from the review. A consultation with the TRB may be scheduled when and as often as needed to benefit from the group's experience and expertise without causing a delay in project progress. The TRB consultation will provide projects with the ability to gain a broader perspective (including insight and linkages with other similar projects, where appropriate) as well as ensure alignment with the enterprise architecture.

5. The XLC Phases, Reviews, and Artifacts

The project's complexity will be used to establish a Project Process Agreement that specifies the artifacts a project will develop, as well as the reviews and tests a project will conduct. It is unlikely that any single project will complete all the artifacts, reviews, and tests. **Table 4** maps the life cycle of possible artifacts to the XLC phases and associated stage gate reviews. For artifacts spanning multiple phases, it is expected that updates to the artifact (usually increased detail reflecting work accomplished in the phase) will be available for review. Artifacts evolve in maturity through the XLC:

- **Preliminary** – The first instance of an artifact that contributes to a stage gate review. The template for each review provides detailed expectations of that particular review.
- **Interim** – A "point-in-time" snapshot of an artifact that contributes to a stage gate review. This updated snapshot should represent progress from the last time the artifact was reviewed. The template for each review provides detailed expectations of that particular review.
- **Baseline** – A version of the artifact that is under initial configuration management control. It is possible but usually difficult to change a baselined artifact. Such a change requires a change request, which ensures that implications to cost, schedule, and technical baselines are addressed. The expectation is that all sections of the artifact have been completed, reviewed, and approved in order to declare a baseline for the artifact.
- **Final** – A baseline version of the artifact that is deemed complete and cannot be changed in later XLC phases. It is deemed unchangeable for a particular release of a system. The expectation is that all sections of the artifact have been completed, reviewed, and approved. A final version of an artifact is used for handoff to Operations and Maintenance (O&M).
- **Updated Continuously** –Security information and artifacts are subject to continuous monitoring and update as needed and/or required.

Table 4. CMS XLC Artifacts by Phase

PHASES	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Testing	Implementation	Operations & Maintenance	Disposition
ARTIFACTS/ INFORMATION **REVIEWS**	AR	ISR	PBR	RR	PDR, DDR	ERR1 (VRR)	ERR2 ERR3 (IRR, PRR)	ORR	PIR, AOA	DR
Acquisition Strategy	P	B								
Project Process Agreement		P/B								
Project Charter		P/F								
Project Management Plan (and/or subsidiary plans)			P/F							
Project Schedule			B	I	I	I	I	F		
Risk Register			P	I	I	I	I	F		
Issues List			P	I	I	I	I	F		
Action Items			P	I	I	I	I	F		
Decision Log			P	I	I	I	I	F		
Lessons Learned Log			P	I	I	I	I	F		
Project Closeout Report									P/F	
System Security Category	P/F									
Privacy Impact Assessment	P	I	I	I	I	I	F		U	
System Security Plan		P	B	I	I	I	F		U	U
Business Risk Assessment		P/F			U				U	U
Information System Risk Assessment		P	I	B	I	I	F		U	U
Information System Description		P	I	I	I	I	B	F	U	U
Security Requirements		P/F							U	
Monitoring Strategy			P/F	U	U	U	U		U	U
Security Control Description				P	B	F	U		U	
Software Assurance Misuse Cases				P	B	I	F		U	
Contingency Plan		P	I	I	I	F	U		U	
Contingency Plan Test							P/F		U	
Security Control Assessment							P	F	U	
ATO Submission								P/F	U	
Plan of Action & Milestones								P/F	U	
CMS CIO-Issued ATO								P/F	U	
Security Monitoring Reports									U	
IT Intake Request Form	P/F									
Enterprise Architecture Analysis Artifacts	P	I	F							
Business Case		P/F								
Requirements Document		P	I	B						
High-Level Technical Design		P/F								
Section 508 Assessment Package		P	I	I	I	I	I	F		
Logical Data Model			P	F						
Release Plan			P	I	F					
System of Records Notice				P	F					
Test Plan				P	I	B				

Artifacts are completed per the Project Process Agreement

Project Management Artifacts	B – Baseline F – Final I – Interim P – Preliminary U – Update Yearly
Security Artifacts	
Security Information from Tasks	
Systems Development Artifacts	

Reviews are conducted per the Project Process Agreement

AR – Architecture Review ISR – Investment Selection Review PBR – Project Baseline Review RR – Requirements Review PDR – Preliminary Design Review DDR – Detailed Design Review	ERR – Environment (Validation, Implementation, Production) Readiness Review ORR – Operational Readiness Review PIR – Post Implementation Review AOA – Annual Operational Analysis DR – Disposition Review

Table 4 (continued): CMS XLC Artifacts by Phase

PHASES	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Testing	Implementation	Operations & Maintenance	Disposition
ARTIFACTS/ INFORMATION **REVIEWS**	AR	ISR	PBR	RR	PDR-DDR	ERR1 (VRR)	ERR2 ERR3 (IRR, PRR)	ORR	PIR AOA	DR
System Design Document					P/B					
Database Design Document					P	F				
Physical Database/Model					P/F					
Interface Control Document					P/B					
Data Use Agreement					P	I	I	F		
Test Case Specification					P	F				
Data Conversion Plan					P	F				
Computer Match Agreement/ Interagency Agreement					P/F					
Implementation Plan					P	I	I	F		
User Manual					P	I	I	F		
Operations & Maintenance Manual					P	I	I	F		
Performance Test Plan and Results Template					P	I	F			
Business Product/Code						P/B				
Version Description Document						P	B			
Training Plan						P/F				
Test Summary Report							P	F		
Training Artifacts							P	F		
System Disposition Plan									P/F	
Post-Implementation Report									P/F	
Annual Operational Analysis Report									P/F	

Artifacts are completed per the Project Process Agreement

Project Management Artifacts						B – Baseline F – Final I – Interim P – Preliminary U – Update Yearly
Security Artifacts						
Security Information from Tasks						
Systems Development Artifacts						

Reviews are conducted per the Project Process Agreement

AR – Architecture Review ISR – Investment Selection Review PBR – Project Baseline Review RR – Requirements Review PDR – Preliminary Design Review DDR – Detailed Design Review	ERR – Environment (Validation, Implementation, Production) Readiness Review ORR – Operational Readiness Review PIR – Post Implementation Review AOA – Annual Operational Analysis DR – Disposition Review

XLC artifacts and their definitions are provided below. Security artifacts and information are listed along with a reference to the Information Security Library which provides definitive information on these subjects.

- **Acquisition Strategy**: The overall objective of an Acquisition Strategy is to document and inform project stakeholders about how the acquisitions will be planned, executed, and managed throughout the life of the project.
- **Action Items**: Records and manages assignments that generally result from meeting discussions.
- **Annual Operational Analysis Report**: Documents elements from the CPIC evaluation and results from monitoring the performance of the system/application during normal operations against original user requirements and any newly implemented requirements or changes. The document assists in the analysis of alternatives for deciding on new functional enhancements and/or modifications to the system/application, or the need to dispose of or replace the system/application altogether.
- **Authorization Package**: The collection of information, serving as evidence that all CMS Minimum Security Requirements are in place, and verified to be operating effectively, that is submitted for inspection and evaluation as parts of the Authorization to Operate process.
- **Business Case**: Describes the basic aspects of the proposed IT project: why, what, when, and how.
- **Business Product/Code**: Documents the implemented system (hardware, software, and trained personnel) that addresses a business need.
- **Business Risk Assessment**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **CMS CIO-Issued Authority to Operate (ATO)**: Provides the required approval, and conditions, authorizing the system to become operational for a specified period. This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **Computer Match Agreement (CMA)/Interagency Agreement (IA)**: Documents agreements permitting computerized comparison of systems of records that contain Personally Identifiable Information.
- **Contingency Plan**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **Contingency Plan Test**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **Data Conversion Plan**: Describes the strategies involved in converting data from an existing system/application to another hardware and/or software environment.
- **Data Use Agreement**: Informs data users of confidentiality requirements and obtains their agreement to abide by these requirements.

- **Database Design Document**: Describes the design of a database and the software units used to access or manipulate that data.
- **Decision Log**: Documents the decisions made over the course of the project.
- **Enterprise Architecture Analysis**: Consists of models, diagrams, tables, and narrative that show the proposed solution's integration into CMS operations from both a logical and technical perspective.
- **High-Level Technical Design**: Documents conceptual functions and stakeholder interactions.
- **Implementation Plan**: Describes how the automated system/application or IT situation will be installed, deployed, and transitioned into an operational system or situation.
- **Information System Description**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **Information Security Risk Assessment**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **Interface Control Document**: Describes the relationship between a source system and a target system. Required for review and normally not updated after originally baselined in the Design Phase.
- **Issues List**: Keeps a record of all issues that occur during the life of a project.
- **IT Intake Form**: Collects basic new project information from a Business Owner.
- **Lessons Learned Log**: Identifies and records lessons learned and future recommendations.
- **Logical Data Model**: Represents CMS data within the scope of a system development project and shows the specific entities, attributes, and relationships involved in a business function's view of information.
- **Monitoring Strategy**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **Operations & Maintenance Manual**: Guides those who maintain, support, and/or use the system in a day-to-day operations environment.
- **Physical Database/Model**: Represents CMS data within the scope of a system development project and shows the specific tables, columns, and constraints involved in a physical implementation's view of information.
- **Plan of Action & Milestones (POA&M)**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **Post-Implementation Report**: Documents results from monitoring the performance of a system/application during normal operations against the original user requirements and any newly implemented requirements or changes.

- **Privacy Impact Assessment**: Ensures that there is no collection, storage, access, use, or dissemination of identifiable respondent information that is not both needed and permitted.
- **Project Charter**: Authorizes the existence of a project and provides the authority to proceed and apply organizational resources.
- **Project Closeout Report**: Assesses the project, ensures completion, and derives lessons learned and best practices to be applied to future projects.
- **Project Management Plan**: Provides detailed plans and schedule, processes, and procedures for managing and controlling the life cycle activities.
- **Project Process Agreement**: Authorizes and documents the justifications for using, not using, or combining specific reviews and the selection of specific work products.
- **Project Schedule**: Shows the Integrated Master Schedule, which includes all activities required to complete a project and their interdependencies.
- **Release Plan**: Describes what portions of the system functionality will be implemented in which release and why.
- **Requirements Document**: Identifies the business and technical capabilities and constraints of the IT project.
- **Risk Register**: Captures the results of a qualitative and quantitative risk analysis and the planned response to those identified risks.
- **Section 508 Assessment**: Provides information regarding compliance with required accessibility standards.
- **Security Control Assessment**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **Security Control Description**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **Security Monitoring Reports**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **Security Requirements**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **Software Assurance Misuse Cases**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **System Design Document**: Documents both high-level system design and low-level detailed design specifications.
- **System Disposition Plan**: Documents how the components of an automated system (software, data, hardware, communications, and documentation) are to be handled at the completion of operations to ensure proper disposition of all the system components and to avoid disruption of the individuals and/or other systems impacted by the disposition.

- **System of Records Notice (SORN)**: Informs the public about a collection of information about its citizens from which data are retrieved by a unique identifier.
- **System Security Category**: This subject is discussed in the Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.
- **System Security Plan**: Documents the system's security level and describes managerial, technical and operational security controls.
- **Test Case Specification**: Describes the purpose of a specific test, identifies the required inputs and expected results, provides step-by-step procedures for executing the test, and outlines the pass/fail criteria for determining acceptance.
- **Test Plan**: Describes the overall scope, technical and management approach, resources, and schedule for all intended test activities associated with validation testing.
- **Test Summary Report**: Summarizes test activities and results, including any variances from expected behavior.
- **Training Artifacts**: Satisfies the training plan with required products, which may include Web-based instruction, instructor guides, student guides, exercise materials, and training records.
- **Training Plan**: Describes the overall goals, learning objectives, and activities that are to be performed to develop, conduct, control, and evaluate instruction.
- **User Manual**: Explains how a novice business user is to use the automated system or application from a business function perspective.
- **Version Description Document**: Identifies, tracks, and controls versions of automated systems and/or applications to be released to the operational environment.

The following sections define each XLC phase and type of review. Depending on the XLC option for Complexity Level 1, 2, or 3 projects, the reviews listed below may be governance or delegated. Risk management tasks integrate with the XLC, are noted here, and are described in detail in the *Risk Management Handbook* (RMH) *Volume I Chapter 1, Risk Management in the XLC* at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

5.1 XLC Phase – Initiation, Concept, and Planning

Overview: During the Initiation, Concept, and Planning Phase, the business owner of an IT solution identifies what the project is intended to do and presents the plans for achieving the business goals and objectives. The activities of this phase include:

- Prepare an IT Intake Request Form
- Identify significant assumptions and constraints, and explore alternatives
- Identify project goals, objectives, risks, and clear and measurable success factors
- Develop an architectural framework and high-level content
- Formally approve the project based on evidence that the business needs will be met and the solution will conform to the Technical Reference Architecture (TRA)
- Analyze how the project will be managed, culminating in the Project Management Plan.

- Develop an acquisition strategy
- Perform the following Risk Management tasks:
  - Security Categorization
  - Information System Description
  - Information System Registration
  - Common Control Identification
  - Security Control Selection
  - Monitoring Strategy
  - Security Plan Approval
- Initiate the Privacy Impact Assessment

Outcomes: The outcomes of the Initiation, Concept, and Planning Phase include:

- Establish the project's feasibility, viability, and alignment with program objectives
- Identify the project's Complexity Level
- Approve all relevant artifacts
- Complete and refine project planning artifacts, including the Project Management Plan, Acquisition Strategy, Project Schedule, and Project Process Agreement baselines.
- Complete security categorization, identification of security controls, and monitoring strategy for the proposed system in accordance with the RMH[2].

5.1.1 Architecture Review (AR)

Purpose: Determine whether the proposed project potentially duplicates, interferes, contradicts, or can leverage another investment that already exists, is proposed, under development, or planned for near-term disposition. The business need is assessed to determine if the IT project is sound and conforms to the CMS Enterprise Architecture.

Project Management Artifacts:

- Acquisition Strategy (Preliminary)

Security Artifacts and Information:

- Privacy Impact Assessment (Preliminary)
- Security Categorization Worksheet (Final)[3]

Systems Development Artifacts:

- Enterprise Architecture Analysis Artifacts (Preliminary)
- IT Intake Form (Final)

[2] The Risk Management Handbook is at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

[3] See RMH Volume II Procedure 2.3 Categorizing an Information System at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

5.1.2 Investment Selection Review (ISR)

Purpose: Determine if the IT project is sound, viable, and worthy of funding, support, and inclusion in the organization's IT Investment Portfolio. The business need and objectives are reviewed to ensure the effort supports CMS' overall mission and objectives and will not compromise initiatives on the horizon. This is an outward-focused review designed to ensure that funding and approval proceed from senior leadership.

Project Management Artifacts:

- Project Charter (Final)
- Project Process Agreement (Baseline)
- Acquisition Strategy (Baseline)

Security Artifacts and Information:

- Business Risk Assessment (Preliminary), with Maximum Tolerable Downtime (Final)
- Security Requirements (Final)
- Contingency Plan (Preliminary)
- Information System Risk Assessment (Preliminary)
- Privacy Impact Assessment (Interim)
- Information System Description (Preliminary)

Systems Development Artifacts:

- Business Case (Final)
- Enterprise Architecture Analysis Artifacts (Interim)
- High Level Technical Design (Preliminary)
- Requirements Document (Preliminary)
- Section 508 Assessment (Preliminary)

5.1.2.1 Project Baseline Review (PBR)

Purpose: Obtain management approval that the scope, cost, and schedule that have been established for the project are adequately documented and that the project management strategy is appropriate for moving the project forward in the life cycle. The PBR includes review of the budget, risk, and user requirements for the investment; emphasis should be on the total cost of ownership and not just development or acquisition costs.

As part of the ongoing overall program risk management process, the following assessments of risk to each baseline should be completed and reported. **Table 5** provides guidelines for initial qualitative assessment appropriate for the PBR. These should be added to any other risks that have been identified and are being tracked by the project.

Project Management Artifacts:

- Action Items, Decision Log, Issues List, and Lessons Learned (Preliminary)
- Project Management Plan (Final)
- Project Schedule (Baseline)

- Risk Register (Preliminary)

Security Artifacts and Information:

- Contingency Plan (Interim)
- Information System Risk Assessment (Interim)
- Privacy Impact Assessment (Interim)
- Information System Description (Interim)
- Monitoring Strategy (Preliminary and Final)

Systems Development Artifacts:

- Enterprise Architecture Analysis Artifacts (Final)
- Logical Data Model (Preliminary)
- Release Plan (Preliminary)
- Requirements Document (Interim)
- Section 508 Assessment (Interim)

Table 5. Risks to Address at the Project Baseline Review

Baseline	Qualitative Risk Assessment	Project Characteristic
Schedule	**High**	Schedule is more than 10% less than estimate based on completed similar effort
	Medium	Schedule is between 5% and 10% less than estimate based on completed similar effort
	Low	Schedule is less than 5% less than estimate based on completed similar effort
Cost	**High**	Estimate At Complete (EAC) exceeds budget by more than 10%
	Medium	EAC exceeds budget between 5% and 10%
	Low	EAC is less than 5% over budget
Technical *contractor experience*	**High**	No experience delivering IT projects for CMS or another HHS department or agency Current Capability Maturity Model Integration assessment is less than 3
	Medium	At least one IT project with CMS or another HHS department or agency Current Capability Maturity Model Integration assessment equals 3

Baseline	Qualitative Risk Assessment	Project Characteristic
	Low	At least three successful IT projects with CMS Current Capability Maturity Model Integration assessment greater than 3
Overall Risk/ Opportunity	**High**	More than five major risks identified and in mitigation
	Medium	Between one and five major risks identified and in mitigation
	Low	No major risks identified or all are currently mitigated

5.2 XLC Phase – Requirements Analysis and Design

Overview: During the Requirements Analysis and Design Phase, a common set of business rules are refined and the business requirements are validated and decomposed into functional and non-functional requirements. The requirements are used to define the design in detail, including inputs, processes, outputs, and interfaces as well as to permit further detailed project management planning. Detailed specifications are developed to support the IT solution that fulfills the requirements for a particular release. The requirements and logical description of the entities, relationships, and attributes of the data are defined and allocated into system and data design specifications. Initial traceability is started between requirements, design, and solution testing. These design specifications are organized specifically to be suitable for implementation and testing within the constraints of a physical environment (e.g., computer, database, and infrastructure).

Perform the risk management tasks described in the *RMH Volume I Chapter 1 Risk Management in the XLC* at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html. The risk management tasks performed during this phase are:

- Security Control Implementation
- Security Control Documentation
- Software Assurance Misuse Case Definition

Outcomes: The outcomes of the Requirements Analysis and Design Phase include:

- Baselined business, functional, and non-functional requirements for release
- Baselined design for the release system components, services, data, security, and infrastructure
- Common repository of business rules, for use by the shared services and all relevant stakeholders.

5.2.1 Requirements Review (RR)

Purpose: Verify that the requirements are complete, accurate, consistent, and problem-free; evaluate the responsiveness to the business requirements; ensure that the requirements are a suitable basis for subsequent design activities; ensure traceability between the business and system requirements; and affirm final agreement regarding the content of the Requirements Document by the business owner.

Project Management Artifacts:

- Action Items, Decision Log, Issues List, and Lessons Learned (Interim)
- Project Schedule (Interim)
- Risk Register (Interim)

Security Artifacts and Information:

- Contingency Plan (Interim)
- Information System Risk Assessment (Baseline)
- Privacy Impact Assessment (Interim)
- Information System Description (Interim)
- Monitoring Strategy (Update)
- Security Control Description (Preliminary)
- Software Assurance Misuse Cases (Preliminary)

Systems Development Artifacts:

- Logical Data Model (Final)
- Release Plan (Interim)
- Requirements Document (Baseline)
- Section 508 Assessment (Interim)
- System of Records Notice (Preliminary)
- Test Plan (Preliminary)

5.2.2 Preliminary Design Review (PDR)

Purpose: Verify that the preliminary design satisfies the functional and nonfunctional requirements and conforms with the CMS TRA; determine the technical solution's completeness and consistency with CMS standards; and raise and resolve any technical and/or project-related issues to identify and mitigate project, technical, security, and/or business risks affecting continued detailed design and subsequent development, testing, implementation, and O&M activities.

Project Management Artifacts:

- Action Items, Decision Log, Issues List, and Lessons Learned (Interim)
- Project Schedule (Interim)
- Risk Register (Interim)

Security Artifacts and Information:

- Contingency Plan (Interim)
- Information Security Risk Assessment (Interim)
- Privacy Impact Assessment (Interim)
- Business Risk Assessment (Update)
- Information System Description (Interim)
- Monitoring Strategy (Update)
- Security Control Description (Baseline)
- Software Assurance Misuse Cases (Baseline)

Systems Development Artifacts:

- Computer Match Agreement/Interagency Agreement (Preliminary)
- Data Conversion Plan (Preliminary)
- Data Use Agreement (Preliminary)
- Database Design Document (Preliminary)
- Implementation Plan (Preliminary)
- Interface Control Document (Preliminary)
- Operations & Maintenance Manual (Preliminary)
- Physical Database/Model (Preliminary)
- Release Plan (Final)
- Section 508 Assessment (Interim)
- System Design Document (Preliminary)
- System of Records Notice (Final)
- Test Case Specification (Preliminary)
- Test Plan (Interim)
- User Manual (Preliminary)

5.2.3 Detailed Design Review (DDR)

Purpose: Verify that the final design satisfies the functional and nonfunctional requirements and conforms with the CMS TRA; determine the technical solution's completeness and consistency with CMS standards; and raise and resolve any technical and/or project-related issues to identify and mitigate project, technical, security, and/or business risks affecting continued detailed design and subsequent development, testing, implementation, and O&M activities. The DDR can be either a delegated review or a governance review with the TRB based on Complexity Level and TRB recommendations:

- For Complexity Level 2 and 3 projects, the DDR is a governance review with the TRB.
- For Complexity Level 1 projects, the DDR is a delegated review.

Project Management Artifacts:

- Action Items, Decision Log, Issues List, and Lessons Learned (Interim)

- Project Schedule (Interim)
- Risk Register (Interim)

Security Artifacts and Information:

- Contingency Plan (Interim)
- Information Security Risk Assessment (Interim)
- Privacy Impact Assessment (Interim)
- Business Risk Assessment (Update)
- Information System Description (Interim)
- Monitoring Strategy (Update)
- Security Control Description (Baseline)
- Software Assurance Misuse Cases (Baseline)

Systems Development Artifacts:

- Computer Match Agreement/Interagency Agreement (Final)
- Data Conversion Plan (Preliminary)
- Data Use Agreement (Preliminary)
- Database Design Document (Preliminary)
- Implementation Plan (Preliminary)
- Interface Control Document (Baseline)
- Operations & Maintenance Manual (Preliminary)
- Physical Database/Model (Final)
- Release Plan (Final)
- Section 508 Assessment (Interim)
- System Design Document (Baseline)
- System of Records Notice (Final)
- Test Case Specification (Preliminary)
- Test Plan (Interim)
- User Manual (Preliminary)

5.3 XLC Phase – Development and Test

Overview: During the Development and Test Phase, the detailed requirements and design information documented in the Requirements Analysis and Design phase are transformed into machine-executable form. The detailed requirements and design information are verified and validated so that all individual system components (and data) of the IT solution function correctly and interface properly with other components within the system.

As necessary, system hardware, networking, telecommunications, and security equipment as well as COTS/Government Off-the-Shelf (GOTS) software are configured. New, custom-software business applications and services are developed, database(s) are built, and software components are integrated.

Test data and test case specifications are finalized, and tests are conducted for individual components, integration, and end-to-end functionality from end-consumer to all systems and back, testing all federal and state agencies, as appropriate, to ensure accurate functionality and data. Tests verify and validate that the IT solution fulfills all business, functional, and non-functional requirements for the release. Formally controlled and focused testing is performed to uncover and prioritize defects in the IT solution that must be resolved. A number of test categories are performed during the Test Phase (e.g., functional testing, integration testing, user acceptance testing, regression testing, and Section 508 testing).

IT solution system components, data, and infrastructure are migrated from a Development environment, to a Test environment, to a Pre-Production/Implementation environment, where applicable. The Pre-Production environment mirrors the Production environment's infrastructure and security configuration management. In this Pre-Production environment, the IT solution undergoes full integration testing from end-consumer to all systems and back, to ensure accurate functionality and data, conduct performance and stress testing, and test for security risks and vulnerabilities. System deployment into this environment is the means to test the use of the Implementation Plan and O&M Manual. All system deployment and configuration management activities are executed as a dry run during this phase, including data conversion. Running the solution in the Pre-Production environment also provides a realistic training environment for users, operators, and maintainers.

Perform the risk management tasks described in the *RMH Volume I Chapter 1 Risk Management in the XLC* at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html. The risk management tasks performed during this phase are:

- Security Control Implementation
- Security Control Documentation
- Software Assurance Misuse Case Definition
- Assessment Preparation

Outcomes: The outcomes of the Development and Test phase include baselined and executable software, infrastructure, database configuration specifications, and test results. Additionally, all IT solution deliverables (executable software, data, configuration files, and documentation) are ready for deployment to the Production environment, and the IT solution is ready for operation.

5.3.1 Environment Readiness Review (ERR)

Purpose: This review combines the three reviews listed below. These reviews are needed to enter the different verification environments to test the solution and its contingency operations. Not all solutions will go through all environments. The environment's owner provides specific requirements for running in each environment.

5.3.1.1 Validation Readiness Review (VRR)

Purpose: Ensure that the system/application completed thorough Development Testing and is ready for turnover to the formal, controlled test environment for Validation Testing.

Project Management Artifacts:

- Action Items, Decision Log, Issues List, and Lessons Learned (Interim)
- Project Schedule (Interim)

- Risk Register (Interim)

Security Artifacts and Information:

- Contingency Plan (Final)
- Information Security Risk Assessment (Interim)
- Privacy Impact Assessment (Interim)
- Information System Description (Interim)
- Monitoring Strategy (Update)
- Security Control Description (Final)
- Software Assurance Misuse Cases (Interim)

Systems Development Artifacts:

- Business Product/Code (Baseline)
- Data Conversion Plan (Final)
- Data Use Agreement (Interim)
- Database Design Document (Final)
- Implementation Plan (Interim)
- Operations & Maintenance Manual (Interim)
- Section 508 Assessment (Interim)
- Test Case Specification (Final)
- Test Plan (Baseline)
- Training Plan (Final)
- User Manual (Interim)
- Version Description Document (Preliminary)

5.3.1.2 Implementation Readiness Rev (IRR)

Purpose: Ensure that the system/application completed thorough Integration Testing and is ready for turnover to the formal, controlled test environment for Production Readiness.

Project Management Artifacts:

- Action Items, Decision Log, Issues List, and Lessons Learned (Interim)
- Project Schedule (Interim)
- Risk Register (Interim)

Security Artifacts and Information:

- Contingency Plan (Update)
- Contingency Plan Test (Preliminary/Final)
- Information System Risk Assessment (Interim)
- Privacy Impact Assessment (Interim)
- Security Control Assessment (Preliminary)

- Information System Description (Interim)
- Monitoring Strategy (Update)
- Security Control Description (Update)
- Software Assurance Misuse Cases (Interim)

Systems Development Artifacts:

- Data Use Agreement (Interim)
- Implementation Plan (Interim)
- Operations & Maintenance Manual (Interim)
- Section 508 Assessment (Interim)
- Test Summary Report (Preliminary)
- Training Artifacts (Preliminary)
- User Manual (Interim)
- Version Description Document (Interim)

5.3.1.3 Production Readiness Review (PRR)

Purpose: Ensure that the infrastructure contractor's operational staff has the appropriate startup and shutdown scripts, accurate application architecture documentation, application validation procedures, and valid contact information to ensure operability of infrastructure applications.

Project Management Artifacts:

- Action Items, Decision Log, Issues List, and Lessons Learned (Interim)
- Project Schedule (Interim)
- Risk Register (Interim)

Security Artifacts and Information:

- Contingency Plan (Update)
- Contingency Plan Test (Final)
- Information Security Risk Assessment (Final)
- Privacy Impact Assessment (Final)
- Security Control Assessment (Preliminary)
- Information System Description (Baseline)
- Monitoring Strategy (Update)
- Security Control Description (Update)
- Software Assurance Misuse Cases (Final)

Systems Development Artifacts:

- Data Use Agreement (Interim)
- Implementation Plan (Interim)
- Operations & Maintenance Manual (Interim)

- Section 508 Assessment (Interim)
- Test Summary Report (Preliminary)
- Training Artifacts (Preliminary)
- User Manual (Interim)
- Version Description Document (Baseline)

5.4 XLC Phase – Implementation

Overview: During the Implementation Phase, the IT solution is put into production based on the Authority to Operate (ATO).

Perform the following Risk Management tasks as described in the *Risk Management Handbook Volume I Chapter 1 Risk Management in the XLC,* located at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html. The Risk Management activities of this phase are:

- Security Control Assessment
- Security Assessment Report
- Remediation Actions
- Plan Of Action And Milestones
- Security Authorization Package
- Risk Determination
- Risk Acceptance

Outcomes: The final IT solution must receive an Authority to Operate (ATO) before deployment to the Production environment.

5.4.1 Operational Readiness Review (ORR)

Purpose: Ensure that the system/application completed its implementation processes according to plan and that it is ready for turnover to the Operations & Maintenance team and operational release into the Production environment.

Project Management Artifacts:

- Action Items, Decision Log, Issues List, and Lessons Learned (Final)
- Project Schedule (Final)
- Risk Register (Final)

Security Artifacts and Information:

- CMS CIO-Issued Authority to Operate (Final)
- Information System Description (Final)
- Security Control Description (Final)
- ATO Submission (Preliminary/Final)
- Plan of Action & Milestones (Final)

Systems Development Artifacts:

- Data Use Agreement (Final)
- Implementation Plan (Final)
- Section 508 Assessment (Final)
- Test Summary Report (Final)
- Training Artifacts (Final)
- User Manual (Final)
- Operations & Maintenance Manual (Final)

5.5 XLC Phase – Operations & Maintenance/Disposition

Overview: After implementation, the IT solution enters the Operations & Maintenance (O&M) Phase. In O&M, the IT solution system components, data, and infrastructure are maintained in the Production environment and monitored to ensure that they continue meeting business needs. All major investments also undergo an Annual Operational Analysis (AOA).

The first review for a new system is performed about six months after entering production and is called a Post-Implementation Review (PIR). The PIR focuses on system performance and lessons learned during the development and implementation of the solution. When a system no longer meets a business need, a Disposition Plan is presented at a Disposition Review (DR) and the system is subsequently retired in accordance with the approved plan.

Perform the following Risk Management tasks as described in the *Risk Management Handbook Volume I Chapter 1 Risk Management in the XLC*, located at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html. The Risk Management activities of this phase are:

- Information System And Environment Changes
- Ongoing Security Control Assessments
- Ongoing Remediation Actions
- Key Updates
- Security Status Reporting
- Ongoing Risk Determination And Acceptance
- Information System Removal And Decommissioning

Outcomes: The outcomes of the O&M/Disposition Phase are that all IT solutions continue meeting business needs safely and securely. Once a solution is deemed obsolete, it is retired and disposed without impacting other operations.

5.5.1 Post-Implementation Review (PIR)

Purpose: The purpose of the PIR is twofold: (1) To ascertain the degree of success from the project; in particular, the extent to which it met its objectives, delivered planned levels of performance, and addressed the specific requirements as originally defined; (2) To enable the team, and future teams, to learn lessons from the project to improve future CMS work and solutions. In that context, the PIR examines whether the team achieved the results it planned for, what those results actually were, and what caused the results to be different from those planned for (if they are different).

Newly-operational systems are required to schedule a Governance-level PIR with the Technical Review Board (TRB) within 6 to 12 months of going into production. Subsequent PIRs (e.g., for each release) should be conducted at the project level (i.e., as a delegated review) unless the system has undergone a total redesign.

Project Management Artifacts:

- Project Closeout Report (Final)

Security Artifacts and Information:

- Privacy Impact Assessment (Update)
- Business Risk Assessment (Update)
- Information System Risk Assessment (Update)
- Information System Description (Update)
- Security Requirements (Update)
- Monitoring Strategy (Update)
- Security Control Description (Update)
- Software Assurance Misuse Cases (Update)
- Contingency Plan (Update)
- Contingency Plan Test (Update)
- Security Monitoring Reports (Update)
- Security Control Assessments (Update)
- ATO Submission (Update)
- Plan of Action & Milestones (Update)
- CMS CIO-Issued Authority to Operate (Update)

Systems Development Artifacts:

- Post-Implementation Report (Final)
- System Disposition Plan (Preliminary)

5.5.2 Annual Operational Analysis (AOA)

Purpose: Evaluate investment performance, user satisfaction with the systems associated with the investment, adaptability to changing business needs, and new technologies that might improve the investment. This review is diagnostic in nature and can lead to development or maintenance activities. Ultimately, the AOA determines whether the IT investment should continue, be modified, or terminated.

Project Management Artifacts:

- N/A

Security Artifacts and Information:

- Privacy Impact Assessment (Update)

- Business Risk Assessment (Update)
- Information System Risk Assessment (Update)
- Information System Description (Update)
- Security Requirements (Update)
- Monitoring Strategy (Update)
- Security Control Description (Update)
- Software Assurance Misuse Cases (Update)
- Contingency Plan (Update)
- Contingency Plan Test (Update)
- Security Monitoring Reports (Update)
- Security Control Assessments (Update)
- ATO Submission (Update)
- Plan of Action & Milestones (Update)
- CMS CIO-Issued Authority to Operate (Update)

Systems Development Artifacts:

- Annual Operational Analysis Report (Final)
- System Disposition Plan (Final)

5.5.3 Disposition Review (DR)

Purpose: Ensure that the IT system has been completely and appropriately transitioned and disposed, thereby ending the life cycle of the IT project.

Project Management Artifacts:

- N/A

Security Artifacts:

- Business Risk Assessment (Update)
- Information System Risk Assessment (Update)
- Information System Description (Update)
- Monitoring Strategy (Update)
- System Retirement Memo (Final)

Systems Development Artifacts:

- N/A

6. Appendix

This appendix includes tables for **sample** Complexity Level 3, 2, and 1 projects that show reviews and associated artifacts. **Every project will vary from these examples** and should follow the Project Process Agreement established for that project.

6.1 Sample Complexity Level 3 Project Reviews and Artifacts

Table 6 lists the artifacts for a **sample** Complexity Level 3 project in preliminary (P), baseline (B), interim (I), and final (F) form as well as the governance and delegated reviews. Section 5 provides the definitions of the phases, reviews, and associated artifacts.

Table 6. Reviews for a Complexity Level 3 Project

Sample Complexity Level 3 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
Initiation, Concept, and Planning	**Architecture Review (AR)**	Governance	**Project Management Artifacts:** • N/A **Security Artifacts and Information:** • Privacy Impact Assessment (P) • Security Categorization Worksheet (F) **Systems Development Artifacts:** • Enterprise Architecture Analysis Artifacts (P) • IT Intake Form (F)
	Investment Selection Review (ISR)	Governance	**Project Management Artifacts:** • Project Charter (F) • Project Process Agreement (B) **Security Artifacts and Information:** • Business Risk Assessment (P), including Maximum Tolerable Downtime (F) • Security Requirements (F) • Contingency Plan (P) • Information System Risk Assessment (P) • Privacy Impact Assessment (I) • Information System Description (P) **Systems Development Artifacts:** • Business Case (F) • Enterprise Architecture Analysis Artifacts (I) • High-Level Technical Design (P) • Requirements Document (P) • Section 508 Assessment (P)
	Project Baseline Review (PBR)	Delegated	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (P) • Project Management Plan (F) • Risk Register (P) **Security Artifacts and Information:** • Contingency Plan (I)

Sample Complexity Level 3 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
			• Information System Risk Assessment (I) • Privacy Impact Assessment (I) • Information System Description (I) • Monitoring Strategy (P/F) **Systems Development Artifacts:** • Enterprise Architecture Analysis Artifacts (F) • Logical Data Model (P) • Project Schedule (B) • Release Plan (P) • Requirements Document (I) • Section 508 Assessment (I)
Requirements Analysis and Design	**Requirements Review (RR)**	Delegated	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **Security Artifacts and Information:** • Contingency Plan (I) • Information System Risk Assessment (B) • Privacy Impact Assessment (I) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (P) • Software Assurance Misuse Cases (P) **Systems Development Artifacts:** • Logical Data Model (F) • Release Plan (I) • Requirements Document (B) • Section 508 Assessment (I) • System of Records Notice (P) • Test Plan (P)
	Preliminary Design Review (PDR)	Governance	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **Security Artifacts and Information:** • Contingency Plan (I) • Information Security Risk Assessment (I) • Privacy Impact Assessment (I) • Business Risk Assessment (U) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (B) • Software Assurance Misuse Cases (B) **Systems Development Artifacts:**

Sample Complexity Level 3 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
			• Computer Match Agreement / Interagency Agreement (P) • Data Use Agreement (P) • Data Conversion Plan (P) • Database Design Document (P) • Implementation Plan (P) • Interface Control Document (P) • Operations & Maintenance Manual (P) • Physical Database/Model (P) • Release Plan (F) • Section 508 Assessment (I) • System Design Document (P) • System of Records Notice (F) • Test Case Specification (P) • Test Plan (I) • User Manual (P)
	Detailed Design Review (DDR)	Governance	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **Security Artifacts and Information:** • Contingency Plan (I) • Information Security Risk Assessment (I) • Privacy Impact Assessment (I) • Business Risk Assessment (U) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (B) • Software Assurance Misuse Cases (B) **Systems Development Artifacts:** • Computer Match Agreement / Interagency Agreement (F) • Data Conversion Plan (P) • Data Use Agreement (P) • Database Design Document (P) • Implementation Plan (P) • Interface Control Document (B) • Operations & Maintenance Manual (P) • Physical Database/Model (F) • Release Plan (F) • Section 508 Assessment (I) • System Design Document (B) • System of Records Notice (F) • Test Case Specification (P) • Test Plan (I) • User Manual (P)

Sample Complexity Level 3 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
Development and Test	**Environment Readiness Review (ERR)**	Delegated	**VRR Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **VRR Security Artifacts and Information:** • Contingency Plan (F) • Information Security Risk Assessment (I) • Privacy Impact Assessment (I) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (F) • Software Assurance Misuse Cases (I) **VRR Systems Development Artifacts:** • Business Product / Code (B) • Data Conversion Plan (F) • Data Use Agreement (I) • Database Design Document (F) • Implementation Plan (I) • Operations & Maintenance Manual (I) • Section 508 Assessment (I) • Test Case Specification (F) • Test Plan (B) • Training Plan (F) • User Manual (I) • Version Description Document (P) **IRR Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **IRR Security Artifacts and Information:** • Contingency Plan (U) • Contingency Plan Test (P/F) • Information System Risk Assessment (I) • Privacy Impact Assessment (I) • Security Control Assessment (P) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (U) • Software Assurance Misuse Cases (I) **IRR Systems Development Artifacts:** • Data Use Agreement (I) • Implementation Plan (I) • Operations & Maintenance Manual (I) • Section 508 Assessment (I) • Test Summary Report (P) • Training Artifacts (P)

Sample Complexity Level 3 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
			• User Manual (I) • Version Description Document (B) **PRR Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **PRR Security Artifacts and Information:** • Contingency Plan (U) • Contingency Plan Test (F) • Information Security Risk Assessment (F) • Privacy Impact Assessment (F) • Security Control Assessment (P) • Information System Description (B) • Monitoring Strategy (U) • Security Control Description (U) • Software Assurance Misuse Cases (F) **PRR Systems Development Artifacts:** • Data Use Agreement (I) • Implementation Plan (I) • Operations & Maintenance Manual (I) • Section 508 Assessment (I) • Test Summary Report (P) • Training Artifacts (P) • User Manual (I) • Version Description Document (B)
Implementation	**Operational Readiness Review (ORR)**	Governance	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (F) • Project Schedule (F) • Risk Register (F) **Security Artifacts and Information:** • CMS CIO-Issued Authority to Operate (FI) • Information System Description (F) • Security Control Description (F) • ATO Submission (Preliminary/FI) • Plan of Action & Milestones (F) **Systems Development Artifacts:** • Data Use Agreement (F) • Implementation Plan (F) • Section 508 Assessment (F) • Test Summary Report (F) • Training Artifacts (F) • User Manual (F) • Version Description Document (B)

6.2 Sample Complexity Level 2 Project Reviews and Artifacts

Table 7 lists the artifacts for a **sample** Complexity Level 2 project in preliminary (P), baseline (B), interim (I), and final (F) form as well as the governance and delegated reviews. Section 5 provides the definitions of the phases, reviews, and artifacts.

Table 7. Reviews for a Complexity Level 2 Project

Sample Complexity Level 2 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
Initiation, Concept, and Planning	**Architecture Review (AR)**	Governance	**Project Management Artifacts:** • N/A **Security Artifacts and Information:** • Privacy Impact Assessment (P) • Security Categorization Worksheet (F) **Systems Development Artifacts:** • Enterprise Architecture Analysis Artifacts (P) • IT Intake Form (F)
	Investment Selection Review (ISR)	Governance	**Project Management Artifacts:** • Project Process Agreement (B) **Security Artifacts and Information:** • Business Risk Assessment (P), including Maximum Tolerable Downtime (F) • Security Requirements (F) • Contingency Plan (P) • Information System Risk Assessment (P) • Privacy Impact Assessment (I) • Information System Description (P) **Systems Development Artifacts:** • Business Case (F) • High-Level Technical Design (P) • Requirements Document (P)
	Project Baseline Review (PBR)	Delegated	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (P) • Project Management Plan (F) • Risk Register (P) **Security Artifacts and Information:** • Contingency Plan (I) • Information System Risk Assessment (I) • Privacy Impact Assessment (I) • Information System Description (I) • Monitoring Strategy (P/F) **Systems Development Artifacts:** • Project Schedule (B) • Release Plan (P) • Requirements Document (I)

Sample Complexity Level 2 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
Requirements Analysis and Design	**Requirements Review (RR)**	Delegated	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **Security Artifacts and Information:** • Contingency Plan (I) • Information System Risk Assessment (B) • Privacy Impact Assessment (I) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (P) • Software Assurance Misuse Cases (P) **Systems Development Artifacts:** • Logical Data Model (F) • Release Plan (I) • Requirements Document (B) • Section 508 Assessment (I) • System of Records Notice (P) • Test Plan (P)
	Preliminary Design Review (PDR)	Governance	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **Security Artifacts and Information:** • Contingency Plan (I) • Information Security Risk Assessment (I) • Privacy Impact Assessment (I) • Business Risk Assessment (U) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (B) • Software Assurance Misuse Cases (B) **Systems Development Artifacts:** • Computer Match Agreement / Interagency Agreement (P) • Interface Control Document (P) • Release Plan (F) • Requirements Document (B) • System Design Document (P) • System of Records Notice (F) Test Plan (I)
	Detailed Design Review (DDR)	Delegated (may be elevated to Governance by TRB)	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **Security Artifacts and Information:**

Sample Complexity Level 2 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
			• Contingency Plan (I) • Information Security Risk Assessment (I) • Privacy Impact Assessment (I) • Business Risk Assessment (U) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (B) • Software Assurance Misuse Cases (B) **Systems Development Artifacts:** • Computer Match Agreement / Interagency Agreement (F) • Implementation Plan (P) • Interface Control Document (B) • Operations & Maintenance Manual (P) • Release Plan (F) • System Design Document (B) • System of Records Notice (F) • Test Case Specification (P) • Test Plan (I) • User Manual (P)
Development and Test	**Environment Readiness Review (ERR)**	Delegated	**VRR Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **VRR Security Artifacts and Information:** • Contingency Plan (F) • Information Security Risk Assessment (I) • Privacy Impact Assessment (I) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (F) • Software Assurance Misuse Cases (I) **VRR Systems Development Artifacts:** • Business Product / Code (B) • Data Use Agreement (I) • Implementation Plan (I) • Operations & Maintenance Manual (I) • Test Case Specification (F) • Test Plan (B) • Training Plan (F) • User Manual (I) • Version Description Document (P) **IRR Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **IRR Security Artifacts and Information:**

Sample Complexity Level 2 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
			• Contingency Plan (U) • Contingency Plan Test (P/F) • Information System Risk Assessment (I) • Privacy Impact Assessment (I) • Security Control Assessment (P) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (U) • Software Assurance Misuse Cases (I) **IRR Systems Development Artifacts:** • Data Use Agreement (I) • Implementation Plan (I) • Operations & Maintenance Manual (I) • Test Summary Report (P) • Training Artifacts (P) • User Manual (I) • Version Description Document (B) **PRR Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **PRR Security Artifacts and Information:** • Contingency Plan (U) • Contingency Plan Test (F) • Information Security Risk Assessment (F) • Privacy Impact Assessment (F) • Security Control Assessment (P) • Information System Description (B) • Monitoring Strategy (U) • Security Control Description (U) • Software Assurance Misuse Cases (F) **PRR Systems Development Artifacts:** • Data Use Agreement (I) • Implementation Plan (I) • Operations & Maintenance Manual (I) • Test Summary Report (P) • Training Artifacts (P) • User Manual (I) • Version Description Document (B)
Implementation	**Operational Readiness Review (ORR)**	Governance	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (F) • Project Schedule (F) • Risk Register (F) **Security Artifacts and Information:** • CMS CIO-Issued Authority to Operate (Fl) • Information System Description (F)

Sample Complexity Level 2 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
			• Security Control Description (F) • ATO Submission (Preliminary/FI) • Plan of Action & Milestones (F) **Systems Development Artifacts:** • Data Use Agreement (F) • Implementation Plan (F) • Test Summary Report (F) • Training Artifacts (F) • User Manual (F) • Version Description Document (B)

6.3 Sample Complexity Level 1 Project Reviews and Artifacts

Table 8 lists the artifacts for a **sample** Complexity Level 1 project in preliminary (P), baseline (B), interim (I), and final (F) form as well as the governance and delegated reviews. Section 5 provides the definitions of the phases, reviews, and artifacts.

Table 8. Reviews for a Complexity Level 1 Project

Sample Complexity Level 1 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
Initiation, Concept, and Planning	**Architecture Review (AR)**	Governance	**Project Management Artifacts:** • N/A **Security Artifacts and Information:** • Privacy Impact Assessment (P) • Security Categorization Worksheet (F) **Systems Development Artifacts:** • IT Intake Form (F)
	Investment Selection Review (ISR)	Governance	**Project Management Artifacts:** • Project Process Agreement (B) **Security Artifacts and Information:** • Business Risk Assessment (P), including Maximum Tolerable Downtime (F) • Security Requirements (F) • Contingency Plan (P) • Information System Risk Assessment (P) • Privacy Impact Assessment (I) • Information System Description (P) **Systems Development Artifacts:** • Business Case (F) • High-Level Technical Design (F) • Requirements Document (P)
	Planning work needed for success in later reviews		**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (P) • Project Management Plan (F) • Project Schedule (B) • Risk Register (P) **Security Artifacts and Information:** • Contingency Plan (I) • Information System Risk Assessment (I) • Privacy Impact Assessment (I) • Information System Description (I) • Monitoring Strategy (P/F) **Information Technology Artifacts:** • N/A
Requirements Analysis and Design	**Preliminary Design Review (PDR)**	Delegated	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I)

Sample Complexity Level 1 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
			Security Artifacts and Information: • Contingency Plan (I) • Information Security Risk Assessment (I) • Privacy Impact Assessment (I) • Business Risk Assessment (U) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (B) • Software Assurance Misuse Cases (B) **Systems Development Artifacts:** • Interface Control Document (P) • Test Plan (P)
	Detailed Design Review (DDR)	Delegated	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (I) • Project Schedule (I) • Risk Register (I) **Security Artifacts and Information:** • Contingency Plan (I) • Information Security Risk Assessment (I) • Privacy Impact Assessment (I) • Business Risk Assessment (U) • Information System Description (I) • Monitoring Strategy (U) • Security Control Description (B) • Software Assurance Misuse Cases (B) **Systems Development Artifacts:** • Interface Control Document (B)
Development and Test	**Development and test work needed for success in later reviews**		**Project Management Artifacts:** • N/A **Security Artifacts and Information:** • Contingency Plan (U) • Contingency Plan Test (F) • Information Security Risk Assessment (F) • Privacy Impact Assessment (F) • Security Control Assessment (P) • Information System Description (B) • Monitoring Strategy (U) • Security Control Description (U) • Software Assurance Misuse Cases (F) **Information Technology Artifacts:** • Business Product / Code (B) • Test Plans (B)
Implementation	**Operational Readiness Review (ORR)**	Governance	**Project Management Artifacts:** • Action Items, Decision Log, Issues List, and Lessons Learned (F) • Project Schedule (F)

Sample Complexity Level 1 Project – Follow your Project Process Agreement			
XLC Phase	**XLC Review**	**Review Type**	**Artifacts**
			• Risk Register (F) **Security Artifacts and Information:** • CMS CIO-Issued Authority to Operate (FI) • Information System Description (F) • Security Control Description (F) • ATO Submission (Preliminary/FI) • Plan of Action & Milestones (F) **Systems Development Artifacts:** • Test Summary Report (F) • Version Description Document (B)