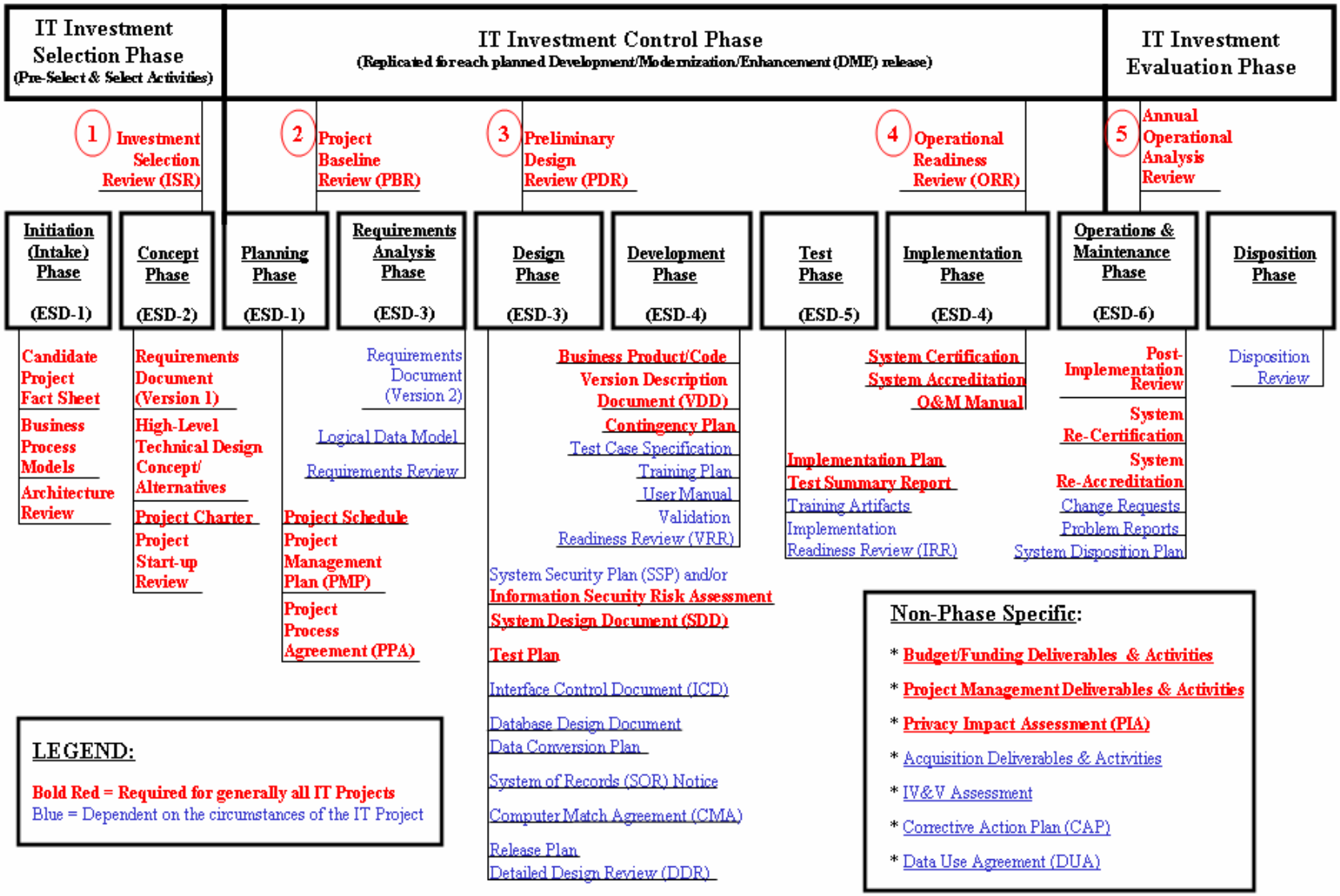
CMS Integrated IT Investment & System Life Cycle Framework (Checkpoints, Deliverables, & Activities)

As of: 3/27/08 9:15 am



CMS Descriptions for Lifecycle Phases

Initiation (Intake) – During the Initiation (Intake) Phase, a business need is identified, the business process is modeled, and a preliminary enterprise architecture review is conducted to determine if there is sufficient justification to proceed into the Concept Phase. The Initiation (Intake) Phase may be triggered by a new investment idea or a proposed major enhancement to an existing investment already in operation. Basic information is collected from the business owner and ostensibly assessed to determine if the proposed investment/project potentially duplicates, interferes, contradicts or can leverage off of another investment/project that already exists, is proposed, is under development, or is planned for near-term disposition. (Maps to Phase 1 of the ESD Services Model)

Concept – During the Concept Phase, high-level analysis and preliminary risk assessment are performed on the proposed investment/project to establish the business case for proceeding forward in the life cycle. Possible business and technical alternatives are identified. High-level system requirements, high-level technical design concept/alternatives and cost estimates are prepared. The Concept Phase ends with a decision by the Information Technology Investment Review Board (ITIRB) of whether or not to commit the necessary resources to solve the business need. (Maps to Phase 2 of the ESD Services Model)

Planning – During the Planning Phase, funds and resources are allocated to the project and the project is officially chartered. Acquisition activities are performed, if necessary, to obtain contractor support. The project work is broken down into specific tasks and sub-tasks, including the identification of project deliverables and assignment of allocated resources to each task. The degree of project management rigor that is to be applied to the project is determined and milestones are established. Specific plans for management and governance of the project are established and documented to guide ongoing project execution and control. The Planning Phase ends with a formal review during which the scope, cost, and schedule baselines for the project are established and approved. (Maps to Phase 1 of the ESD Services Model)

Requirements Analysis – During the Requirements Analysis Phase, the business (project in-scope) requirements that were previously documented in an earlier phase are revalidated and further analyzed and decomposed into high-level system (functional and nonfunctional) requirements that define the automated system/application in more detail with regard to inputs, processes, outputs, and interfaces. If appropriate, a logical depiction of the data entities, relationships and attributes of the system/application is also created. During the Requirements Analysis Phase, the initial strategy for testing and implementation is also begun. In addition, the work planned for future phases is redefined, if necessary, based on information acquired during the Requirements Analysis Phase. The Requirements Analysis Phase ends with a review to determine readiness to proceed to the Design Phase. (Maps to Phase 3 of the ESD Services Model)

Design – The Design Phase seeks to develop detailed specifications that emphasize the physical solution to the user's information technology needs. The system requirements and logical description of the entities, relationships, and attributes of the data that were documented during the Requirements Analysis Phase are further refined and allocated into system and database design specifications that are organized in a way suitable for implementation within the constraints of a physical environment (e.g., computer, database, facilities). A formal review of the high-level architectural design is conducted prior to detailed design of the automated system/application to achieve confidence that the design satisfies the system requirements, is in conformance with the enterprise architecture and prescribed design standards, to raise and resolve any critical technical and/or project-related issues, and to identify and mitigate project, technical, security, and/or business risks affecting continued detailed design and subsequent lifecycle activities. During the Design Phase, the initial strategy for any necessary training is also begun. Estimates of project expenses are updated to reflect actual costs and estimates for future phases. In addition, the work planned for future phases is redefined, if necessary, based on information acquired during the Design Phase. (Maps to Phase 3 of the ESD Services Model)

Development – During the Development Phase, the system developer takes the detailed logical information documented in the previous phase and transforms it into machine-executable form, and ensures that all of the individual components of the automated system/application function correctly and interface properly with other components within the system/application. As necessary and appropriate, system hardware, networking and telecommunications equipment, and COTS/GOTS software is acquired and configured. New custom-software programs are developed, database(s) are built, and software components (COTS, GOTS, and custom-developed software and databases) are integrated. Test data and test case specifications are finalized. Unit and integration testing is performed by the developer with test results appropriately documented. Data conversion and training plans are finalized and user procedures are baselined, while operations, office and maintenance procedures are also initially developed. The Development Phase ends with a review to determine readiness to proceed to the Test Phase. (Maps to Phase 4 of the ESD Services Model)

Test – The primary purpose of the Test Phase is to determine whether the automated system/application software or other IT solution developed or acquired and preliminarily tested during the Development Phase is ready for implementation. During the Test Phase, formally controlled and focused testing is performed to uncover errors and bugs in the IT solution that need to be resolved. There are a number of specific validation tests that are performed during the Test Phase (e.g., requirements validation, system integration, interface, regression, security, performance, stress, usability, and user acceptance). Additional tests may be conducted to validate documentation, training, contingency plans, disaster recovery, and installation depending upon the specific circumstances of the project. The Test Phase ends with a review to determine readiness to proceed to the Implementation Phase. (Maps to Phase 5 of the ESD Services Model)

Implementation – During the Implementation Phase, the automated system/application or other IT solution is moved from development status to production status. The process of implementation is dependent on the characteristics of the project and the IT solution, and thus may be synonymous with installation, deployment, rollout, or go-live. If necessary, data conversion, pilot testing, and training for using, operating, and maintaining the system are accomplished during the Implementation Phase. From a system security perspective, the final system must be certified and accredited for use in the production environment during the Implementation Phase. The Implementation Phase ends with a formal decision to release the final IT solution into the Operations and Maintenance Phase. (Maps to Phase 4 of the ESD Services Model)

Operations & Maintenance – During the Operations & Maintenance Phase, the certified and accredited system is released into the full-scale production environment for sustained use and operations/ maintenance support. Changes and problems with the automated system/application or other IT solution may continually be identified and resolved to ensure that the system/application or other technological solution meets ongoing functional and non-functional needs. Periodically the automated system/ application will also need to be re-certified and re-accredited for continued operation in the production environment. When the time comes that the automated system/application or other technological solution will no longer be needed or will be replaced, then a plan for final disposition of the system/application or IT solution must be prepared and approved prior to moving into the Disposition Phase. (Maps to Phase 6 of the ESD Services Model)

Disposition – During the Disposition Phase, the operation of an automated system/application or other IT solution is formally ended in accordance with organization needs and pertinent laws and regulations. The automated system/application or other IT solution is retired or disposed of based on the formal disposition plan approved during the Operations & Maintenance Phase. The disposition activities ensure the orderly termination of the automated system/application and preserve vital information about the system so that some or all of the information may be reactivated in the future if necessary. Particular emphasis is given to proper preservation of the data processed by the system/application, so that the data is effectively migrated to another system/application or archived in accordance with applicable records management regulations and policies for potential future access.

CMS Mapping of Artifacts/Deliverables to Lifecycle Phases

Artifact/Deliverable	Description	Status *	Template Exists	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
Candidate Project Fact Sheet	The Candidate Project Fact Sheet identifies the name and owner of the proposed project, identifies the nature of the project (new project versus enhancement), provides a brief description of the investment/project (i.e., purpose/goals and scope), identifies any legislative or regulatory mandates/ requirements the project will support, identifies the organizations, components, or groups impacted by the effort (including internal and external entities), explains the types of data that will be used in the investment/project, and identifies if the project is believed to involve the exchange or storage of personally identifiable information and/or sensitive information.	M	Y												
Business Process Models (BPMs)	The BPMs and companion narrative communicate the scope, business alternatives (build, buy, modify), and business risk assessment to the primary stakeholders to achieve understanding and buy-in and to assist the Information Technology Investment Review Board (ITIRB) in making an informed funding decision for the IT investment/project.	M	Y												
Requirements Document	The Requirements Document identifies the business and technical capabilities and constraints of the IT project or automated system/application to be developed. The primary purpose of the Requirements Document is to clearly communicate the goals, needs, and objectives of the user(s) and/or business organization (i.e., customer requirements) to the technical community who will specify and build the end product (e.g., automated system/application or other IT solution). The Requirements Document provides a basis for design, and serves as a foundation for testing and user acceptance of the end product. The first version of the Requirements Document created during the Concept Phase includes business requirements, which are statements of the functions or program needs that must be met in order to accomplish the business objectives of the IT project (in-scope requirements for the project). Also included are high-level functional and nonfunctional requirements that further define the expectations for the end product. Functional requirements are actions or expectations of what the automated system/application will take or do, and are measured by concrete means like data values, decision-making logic and algorithms. Nonfunctional requirements are behavioral properties that the automated system/application must have. During the Requirements Analysis Phase, the high-level functional and nonfunctional requirements are revalidated and further analyzed and refined into lower-level, more-detailed system requirements.	M	Y												
High-Level Technical Design Concept/Alternatives	The High-Level Technical Design Concept/Alternatives provides an analysis that bridges the gap between the users' operational needs and the developer's technical alternatives, without becoming bogged down in detailed technical issues that are addressed during requirements analysis and design activities. The artifact documents the possible technical alternatives, along with the associated rationale, estimated full costs and risk assessment to assist the ITIRB in making an informed funding decision.	M	Y												
Project Charter	The Project Charter is a document that formally authorizes the existence of a project, and provides the authority to apply organizational resources to project activities.	M	Y												
Project Schedule	The Project Schedule documents the planned dates for performing the tasks and for meeting the milestones that comprise a project. The Project Schedule includes identification of anticipated task durations, resources assigned to the tasks, and relationships to predecessor and successor tasks.	M	Y												

* M= Mandatory; CM=Conditionally Mandatory

Artifact/Deliverable	Description	Status *	Template Exists	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
Project Management Plan (PMP)	The PMP provides detailed plans, processes, and procedures for managing and controlling the life cycle activities of a specific IT project. The PMP describes the processes for managing, tracking, and controlling the development of an automated system/application or other IT solution. It provides necessary information to improve the level of communication and understanding between all project team members and stakeholders, and may be comprised of other subsidiary management plans.	M	Y												
Project Process Agreement (PPA)	The PPA is used to authorize and document the justifications for using, not using, or combining specific stage gate reviews and the selection of specific deliverables applicable to the investment/project, including the expected level of detail to be provided.	M	Y												
Logical Data Model (LDM)	A LDM is a graphical representation that provides the definition, characteristics, and relationships of data for a business function. Its purpose is to describe end-user data to systems staff. It provides a definition of the entities, relationships and attributes that are used by a system.	CM	N												
System Security Plan (SSP)	As required by the Federal Information Security Management Act (FISMA) of 2002, all information systems that store or process sensitive information must be covered by a SSP. The SSP contains descriptions of the actual managerial, technical and operational controls, documenting the current level of security implemented within the system. CMS has established a hierarchical structure for the development of SSPs. At the highest level is the CMS Master Security Plan, which defines the enterprise-level security controls that are in place within CMS. The Master Security Plan documents all of the security attributes that are standard enterprise-wide (e.g., personnel controls, overarching physical controls for the CMS site, contingency planning and disaster recovery, etc.). All lower-level SSPs inherit the attributes of the Master Security Plan, unless otherwise documented in that lower-level SSP. Subordinate to the Master Security Plan are SSPs for each General Support System (GSS), which document all the security attributes of a specific GSS (e.g., review of security controls, physical and environmental protection specific to the GSS, production input/output, etc.). A GSS is a grouping of systems that consist of interconnected information resources under the same direct management control that share common functionality. A GSS normally includes hardware, software, information, data, applications, communications, facilities, and provides general support for a variety of users and/or applications. As a rule of thumb, a GSS is a physical platform and infrastructure upon which applications run (e.g., mainframe systems, web servers, communications equipment, etc.). Subordinate to the GSS SSPs are SSPs for each of the established Major Applications (MA). A MA is a grouping of CMS application systems that support clearly defined business functions for which there are readily identifiable security considerations and needs. A MA is usually comprised of multiple application systems and occasionally might have hardware, software, and telecommunication components. These components can be a single software application or a combination of hardware/software focused on supporting a specific business-related function. MA SSPs only need to document the security controls specific to the MA and how, if applicable, their system adds to or deviates from the controls supported by the higher-level GSS and/or Master Plan.	CM	Y												

* M= Mandatory; CM=Conditionally Mandatory

Artifact/Deliverable	Description	Status *	Template Exists	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
Information Security Risk Assessment (IS RA)	An IS RA must be prepared for each GSS, GSS sub-system (if applicable), MA and MA application. The IS RA contains a list of system threats and vulnerabilities, an evaluation of current system security controls, their resulting risk levels, and any recommended safeguards to reduce the system's risk exposure. The IS RA also supports risk management through the evaluation of the system's risk impact upon the enterprise security model.	M	Y												
System Design Document (SDD)	The SDD describes how the system requirements recorded in the Requirements Document, preliminary functional and technical design recorded in the BPMs and High-Level Technical Design Concept/Alternatives, and the preliminary data design documented in the LDM are transformed into more technical system design specifications from which the system will be built. The SDD is used to document both high-level system design and low-level detailed design specifications, and is typically created in two increments. The first increment of the SDD describes design goals and considerations, provides a high-level overview of the system architecture and data design for the system, as well as the human-machine interface and concept of execution. This version of the SDD serves as the primary input to the Preliminary Design Review (PDR). In conjunction with the Interface Control Document (ICD), if required, the SDD describes completely the external interfaces with other systems and/or entities and provides capacity planning estimates for infrastructure resources. In the second increment of the SDD, modifications are made to the high-level design, if necessary, based on the results of the PDR. The high-level system design is further decomposed into low-level detailed design specifications for each of the system's internal components, including hardware, communications, software, system integrity controls, and interfaces. The SDD also includes a Requirements Traceability Matrix and a Section 508 Product Assessment.	M	Y												
Section 508 Product Assessment	The Section 508 Product Assessment is the mechanism for providing information regarding an electronic and information technology (EIT) product's compliance with the accessibility standards set forth by the Federal Access Board, which are the technical and functional provisions and performance criteria by which compliance with Section 508 of the Rehabilitation Act of 1973, as amended, are determined.	M	Y												
Interface Control Document (ICD)	An ICD describes the relationship between a source system and a target system. The ICD governs the data exchanged between the two systems and provides information describing the data exchange syntax and semantics that have been agreed upon for use. ICDs can also be used for subsystems, hardware configuration items, Computer Software Configuration Items (CSCIs), manual operations, and other system components. The ICD establishes the data exchange content, format, communications protocol, transmission mechanism, security provisions, triggering events, timing, as well as any constraints that govern information exchange between the two systems.	CM	Y												
Database Design Document	The Database Design Document describes the design of a database and the software units used to access or manipulate the data. It is used as the basis for implementing the database and related software units. It also provides information needed to support database administration.	CM	Y												

* M= Mandatory; CM=Conditionally Mandatory

Artifact/Deliverable	Description	Status *	Template Exists	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
Data Conversion Plan	A Data Conversion Plan is required for all migration projects, regardless if it is a project to replace a COTS business application or to port an existing in-house custom-developed system/application to a new platform. A Data Conversion plan describes the strategies involved in converting data from an existing system/application to another hardware and/or software environment. It includes an inventory and cross reference of source and target data elements, schema, metadata and all self-describing files; process for data extraction, transformation and loading for each data source; tools needed to execute the conversion; and strategy for data quality assurance and control.	CM	Y												
Release Plan	If the project is utilizing releases in its development and implementation approach, a Release Plan describes what portions of the system functionality will be implemented in which releases and the rationale for each release.	CM	Y												
System of Records (SOR) Notice	The Privacy Act defines a SOR as a group of any records under the control of a Federal agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Additionally, the Privacy Act requires that the Federal government inform the public of any collection of information about its citizens from which data are retrieved by a unique identifier as described above. The SOR Notice fulfills this requirement to inform the public via the publication of a system notice in the *Federal Register*. This notice describes the SOR and gives the public an opportunity to comment. Without the written consent of the subject individual, the Privacy Act prohibits the release of protected information maintained in a SOR unless one of the 12 disclosure exceptions is applicable. A SOR Notice consists of three documents: a Narrative Statement that is submitted to the Office of Management & Budget (OMB), and a Preamble and Statement of Records Notice that are provided to Congress. The Preamble and the Statement of Records Notice are also published in the *Federal Register* to notify the public of a new or revised SOR.	CM	Y												
Computer Match Agreement (CMA)	A CMA is a written accord that establishes the conditions, safeguards, and procedures under which a Federal organization agrees to disclose data where there is a computerized comparison of two or more automated System of Records (SORs). A "matching program" is any computerized comparison of two or more SORs, or a SOR with non-Federal records for the purpose of (1) establishing or verifying eligibility or compliance with law or regulations of applicants or recipients / beneficiaries, or (2) recouping payments or overpayments. The definition also encompasses matches involving Federal personnel or payroll records. In conjunction with a CMA, an Inter/Intra-agency Agreement (IA) is also prepared when the SOR(s) involved in the comparison are the responsibility of another Federal agency.	CM	Y												
Inter/Intra-agency Agreement (IA)	An IA, also known as a reimbursable agreement, is a written accord in which a Federal agency agrees to provide to, purchase from, or exchange with another Federal agency services, supplies, or equipment. An IA is the document with which the receiving agency agrees to reimburse the providing agency for the cost of the services, supplies, or equipment. In certain cases two or more agencies may agree to exchange services, supplies, or equipment without a transfer of funds. Although an IA is usually between two agencies, occasionally, an IA may involve more than two agencies.	CM	Y												

* M= Mandatory; CM=Conditionally Mandatory

Artifact/Deliverable	Description	Status *	Template Exists	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
Memorandum of Understanding (MOU)	In contrast to an IA, a MOU is another instrument used when agencies enter into a joint project in which they each contribute their own resources; in which the scope of work is very broad and not specific to any one project; or in which there is no exchange of goods or services between the participating agencies.	CM	Y												
Contingency Plan	The Contingency Plan describes the strategy for ensuring system recovery in accordance with stated recovery time and recovery point objectives.	M	N												
Business Product/ Code	The Business Product is the primary result from the development effort that satisfies the established requirements. In software development efforts, it includes the original source code and machine-compiled, executable computer instructions, and data repository(ies).	M	N												
Version Description Document (VDD)	The VDD is the primary configuration control document used to track and control versions of software being released to testing, to implementation, or to the final operational environment. The VDD provides a summary of the features and contents for a specific software build or release, and facilitates product implementation, testing, operations and maintenance. The VDD identifies and describes the version of the computer software configuration items (CSCIs) that comprise the software build or release, including all changes to the CSCIs since the last VDD was issued, as well as installation and operating information unique to the version described. The VDD applies to any release of a product revision, and includes software, hardware, and firmware.	M	Y												
Implementation Plan	The Implementation Plan describes how the automated system/application or IT situation will be installed, deployed and transitioned into an operational system or situation. The plan contains an overview of the system or situation, a brief description of the major tasks involved in the implementation, and the overall resources needed to support the implementation effort (e.g., hardware, software, facilities, materials, and personnel). If the implementation is to occur at multiple locations, the overall sequence and site-specific implementation specifications are also documented.	M	Y												
Test Plan	The Test Plan describes the overall scope, technical and management approach, resources, and schedule for all intended test activities associated with validation testing. The Test Plan describes the items to be tested, the testing tasks to be performed, the personnel responsible for each task, the schedule and required resources for the testing activities, and the risks associated with the test plan that require contingency planning. The test plan should take into account security test and evaluation (ST&E), Section 508 compliancy, and any potential impact to the infrastructure.	M	Y												
Test Case Specification	A 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.	CM	Y												
Test Summary Report	A Test Summary Report is completed at the end of testing to document the results. It summarizes the testing activities that were performed during the development of a system or system release. It describes any variances between the testing that was *planned* and the testing that actually *occurred*. It also provides a summary of the test results that were achieved from the testing, as well as provides an evaluation of the test items. This includes identification of significant problems or defects that were encountered and resolved during testing, their corresponding resolutions, as well as any unresolved problems or defects that were encountered and a plan of action for their resolution. It also details each test case executed with the date it was tested and by whom, and whether the test case passed or failed based upon the acceptance criteria.	M	Y												

* M= Mandatory; CM=Conditionally Mandatory

Artifact/Deliverable	Description	Status *	Template Exists	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
Training Plan	The Training Plan describes the overall goals, learning objectives, and activities that are to be performed to develop, conduct, control, and evaluate instruction that is to be provided to users, operators, administrators, and support staff who will use, operate, and/or otherwise support an automated system/application or other IT solution.	CM	Y												
Training Artifacts	Training Artifacts include instructor and student guides, audio-visual aids, and computer-based or web-based software used to disseminate information about an automated system/application or other IT solution to the target audience that is in need of the instruction.	CM	N												
User Manual	The User Manual clearly explains how a novice business user is to use the automated system or application from a business function perspective. The User Manual is usually organized topically or by task.	CM	Y												
Operations & Maintenance (O&M) Manual	The O&M Manual clearly describes the automated system or application that will be operating in the production environment and provides the operations and support staff with the information necessary to effectively handle routine production processing, ongoing maintenance, and identified problems/issues. The O&M Manual describes the operational system and its stakeholders, as well as the roles and responsibilities for ongoing operations and maintenance of the system. It describes the sources of software components and other assets, how the architecture was implemented, the use of the architecture and assets, and how it is to be maintained. The O&M Manual provides documented procedures for performing tasks associated with equipment administration, network administration, application administration, and system administration, as well as data and database administration.	M	Y												
Service Level Agreement (SLA)	A SLA is a contractual agreement between a service provider and their customer specifying performance guarantees with associated penalties should the service not be performed as contracted.	CM	Y												
Change Request(s)	A Change Request (CR) is a formal document used to request a modification to specified software components, hardware, or documents that is managed through an established change control process. A CR may be initiated anytime after a baseline has been established.	CM	Y												
Problem Report(s)	A Problem Report (PR) is a formal document used to record an unexpected result that occurs during formal testing, implementation, or operation of the specified software or hardware. A PR is managed through an established process that includes investigation, resolution, and verification.	CM	Y												
System Disposition Plan	The System Disposition Plan addresses how the various 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.	CM	Y												

* M= Mandatory; CM=Conditionally Mandatory

Artifact/Deliverable	Description	Status *	Template Exists	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
Budget/Funding Artifacts & Activities - Exhibit 300 (a.k.a., OMB Capital Asset Plan & Business Case Summary)	The Exhibit 300 is an annual document required by the Office of Management & Budget (OMB), which refers to the requirements described in Section 300 of the OMB Circular A-11. The information provided in the Exhibit 300 justifies new or continued funding for a "Major" IT investment/ project by demonstrating a direct connection to the President's Management Agenda, the Department of Health & Human Services (DHHS) Strategic Goals, the applicable HHS OPDIV Strategic Plan, positive return on investment, sound acquisition planning, risk mitigation and management planning, realistic cost and schedule goals, measurable performance benefits, and adherence to architecture, security, and privacy standards. The Exhibit 300 contains three major sections: 1) a summary of spending by fiscal year for planning, acquisition, and maintenance activities; 2) justification, alternatives, and risks; and 3) original baseline and current cost, schedule, and performance goals. An initial Exhibit 300 is prepared based on the results of the Concept Phase. In subsequent years, there is a focus on the third section of the Exhibit 300 comparing the baseline information with the current project status.	CM	Y												
Acquisition Artifacts & Activities	Includes: • Request for Contract (RFC) • Statement of Work (SOW) / Task Order • Inter/Intra-agency Agreement (IA) • HHS-393 Form • Section 508 Product Assessment	CM	Y												
Project Management Artifacts & Activities	Includes: • Integrated Baseline Artifacts • Contractor Performance Report (CPR) • Closeout Certifications • Meeting Minutes • Updated Project Schedule • Project Dashboard Reports • Risk Report	M	Y												
Privacy Impact Assessment (PIA)	The E-Government Act of 2002, Section 208 (Public Law 107-347, 44 U.S.C., Ch 36) requires Federal agencies to conduct a Privacy Impact Assessment (PIA) when "developing or procuring information technology . . . or initiating a new collection of information . . . in an identifiable form . . . " The purpose of a PIA is to ensure there is no collection, storage, access, use or dissemination of identifiable respondent information (i.e., identifiable data about both people and businesses) that is not both needed and permitted. A PIA is a program analysis of how collected information is handled by the agency to determine whether the data collected are protected in a manner consistent with Federal standards for privacy and security. The PIA determines what kind of information in identifiable form is contained within a system, what is done with that information, and how that information is protected. In addition to being required by the E-Government Act of 2002, PIAs are required by Office of Management and Budget (OMB) Circular No. A-11 and OMB Exhibit 300, "Capital Asset Plan and Business Case," which tie together privacy considerations and executive agency funding requests. Though the PIA specifically refers to "privacy", a PIA also typically covers confidentiality, access to data, and use of data. A PIA is organized around four Privacy Principles: 1) mission necessity, 2) informed consent, 3) protection from unwarranted intrusion, and 4) protection of confidentiality.	M	Y												

* M= Mandatory; CM=Conditionally Mandatory

Artifact/Deliverable	Description	Status *	Template Exists	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
Corrective Action Plan (CAP)	A CAP is used to track the status of a Security Test & Evaluation (ST&E) finding or an audit finding. A CAP provides a brief description of a finding, including the risk level (high, medium, or low) and the scheduled closing date, as well as other information pertaining to the finding. This information is recorded in a CAP Management Worksheet, also known as a Plan of Action and Milestones (POA&M).	CM	Y												
Data Use Agreement (DUA)	A DUA is a legal binding agreement between a Federal agency and an external entity (e.g., contractor, private industry, academic institution, other Federal government agency, or state agency), when an external entity requests the use of personal identifiable data that is covered by the Privacy Act of 1974. The agreement delineates the confidentiality requirements of the Privacy Act, security safeguards, and the Federal agency's data use policies and procedures. The DUA serves as both a means of informing data users of these requirements and a means of obtaining their agreement to abide by these requirements. Additionally, the DUA serves as a control mechanism through which the Federal agency can track the location of its data and the reason for the release of the data. A DUA requires that a System of Records (SOR) Notice be in effect, which allows for the disclosure of the data being used.	CM	Y												

CMS Mapping of Reviews to HHS EPLC Lifecycle Phases

Review	Description	Status *	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
Architecture Review	The Architecture Review is a high-level, preliminary enterprise architecture assessment that is performed during the intake process, which results in a pre-selection decision to either move forward into the Concept Phase of the lifecycle for what appears to be a promising IT investment/ project or to end the lifecycle at this point for the proposed IT investment/project.	M												
Project Start-up Review	The Project Start-up Review is an enterprise architecture assessment that is performed by the Technical Review Board (TRB) to provide advice on significant architectural decisions before a system development/integration contractor is procured.	M												
Investment Selection Review (ISR)	The ISR is a formal inspection of a proposed IT investment/project by the Information Technology Investment Review Board (ITIRB) to determine if it is a sound, viable investment/project worthy of funding, support and inclusion in the agency's IT Investment Portfolio.	M												
Project Baseline Review (PBR)	The PBR is a formal inspection of the entire project and performance measurement baseline initially developed for the IT investment/project. The PBR is conducted to 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. Upon successful completion of this review, the Project Schedule and Project Management Plan are officially baselined.	M												

* M= Mandatory; CM=Conditionally Mandatory

Review	Description	Status *	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
Requirements Review	The Requirements Review is conducted to verify that the requirements are complete, accurate, consistent and problem-free; to evaluate the responsiveness of the requirements to the business requirements; to ensure that the requirements are a suitable basis for subsequent design activities; to ensure traceability within the requirements and between the design documents; and to affirm final agreement regarding the content of the Requirements Document. Upon successful completion of this review, the Requirements Document is baselined.	CM												
Preliminary Design Review (PDR)	The PDR is a formal inspection of the high-level architectural design of an automated system, its software and external interfaces, which is conducted to achieve agreement and confidence that the design satisfies the functional and nonfunctional requirements and is in conformance with the enterprise architecture. Overall project status, proposed technical solutions, evolving software products, associated documentation, and capacity estimates are reviewed to determine completeness and consistency with design standards, to raise and resolve any technical and/or project-related issues, and to identify and mitigate project, technical, security, and/or business risks affecting continued detailed design and subsequent development, testing, implementation, and operations & maintenance activities.	M												
Detailed Design Review (DDR)	A DDR is conducted subsequent to a PDR to achieve confidence that the individual design components (units/modules) of an automated system/application, and how they interface with one another, have been completely defined and documented in sufficient detail such that the design of the automated system/application is complete, fully integrated, and ready to move to the Development Phase. Upon successful completion of this review, the SDD and other adjunct documents are baselined.	CM												
Validation Readiness Review (VRR)	The VRR is conducted to provide assurance that the software that is about to enter validation (system) testing has completed thorough unit/module/software integration testing during the development of the automated system/application and is ready for turnover to the formal, controlled test environment where validation testing will be conducted. The scope of the VRR is to inspect the test products and test results obtained during development testing for completeness and accuracy, and to verify that test planning, test cases, scenarios, and scripts provide adequate coverage of documented system requirements. In addition, a review of the test environment, test setup, and test data is performed to ensure they are adequately prepared for validation testing.	CM												
Implementation Readiness Review (IRR)	The IRR is conducted to ensure that the IT solution or automated system/application that has been developed is ready for implementation activities, such that the required system hardware, networking and telecommunications equipment; COTS, GOTS, and/or custom-developed software; and database(s) can be installed and configured in the production environment(s).	CM												

* M= Mandatory; CM=Conditionally Mandatory

Review	Description	Status *	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
System Certification	System Certification is the comprehensive evaluation of the management, operational, and technical security controls implemented for an information system to ensure compliance with information security requirements. The certification evaluation includes review of the IS RA, SSP, other system life cycle documentation, and any findings from past assessments, reviews and/or audits, as well as technical testing and analysis. The technical certification assessment, called the Security Test and Evaluation (ST&E) process, is the execution of test procedures and techniques by an independent third party designed to evaluate the effectiveness of information security controls in a particular environment, and to identify any vulnerabilities in the information system. The results of the certification assessment, together with a review of any other independent audits, reviews or assessments are documented and appropriate corrective action is taken to strengthen internal controls. The SSP and/or IS RA are then updated based upon improvements and changes made to the system, and then the system is certified (approved) prior to subsequent System Accreditation (i.e., authorization to process) by the CMS Chief Information Officer/ Designated Approval Authority.	M												
System Accreditation	System Accreditation is the official management decision to authorize operation of an information system. To make an informed decision, the Chief Information Officer (CIO) / Designated Approval Authority (DAA) must have sufficient knowledge and understanding of the current status of the security programs and security controls in place to protect the system and information processed, stored, or transmitted by the system. This is a business-driven, risk-based decision founded upon current, credible, comprehensive documentation and test results provided in the System Certification package prepared as a result of predecessor System Certification activities. The CMS CIO/DAA must explicitly accept or reject any identified residual risks to CMS operations and assets remaining after the implementation of the prescribed set of security controls as documented in the SSP and/or IS RA. Ultimately, the CIO/DAA must strike a firm balance between authorizing the operation of information systems necessary to support completion of the business mission, while ensuring that an adequate level of information security is in place. The objective is to strive to implement the most effective security controls, in consideration of technical, budgetary, time, and resource limitations, while continuing to support business mission requirements.	M												
Operational Readiness Review (ORR)	The ORR is a formal inspection conducted to determine if the final IT solution or automated system/application that has been developed or acquired, tested, and implemented is ready for release into the production environment for sustained operations and maintenance support.	M												
Annual Operational Analysis Review	The Annual Operational Analysis Review is a diagnostic inspection conducted to evaluate system performance, user satisfaction with the system, adaptability to changing business needs, and new technologies that might improve the system. This analysis ultimately determines whether the IT investment should continue as is, be modified, or terminated.	M												

* M= Mandatory; CM=Conditionally Mandatory

Review	Description	Status *	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	O&M	Disposition	Annual	Recurring or As Needed
Post -Implementation Review (PIR)	After a period of sustained operation (after at least one full processing and reporting cycle has been completed and all users have been trained and are comfortable with the operation), a PIR is conducted of the completed IT solution or automated system/application that was released into the production environment to determine if it is operating as expected. The purpose of the review is to ascertain the degree of success from the project (in particular, the extent to which it met its objectives, delivered planned levels of benefit, and addressed the specific requirements as originally defined), to examine the efficacy of all elements of the working business solution to see if further improvements can be made to optimize the benefit delivered, and to learn lessons from the project that can be used to improve future project work and solutions.	M												
System Re-Certification	System Re-Certification is the comprehensive re-evaluation of the management, operational, and technical security controls implemented for an information system that is performed during the Operations & Maintenance Phase to ensure that the system is continuing to operate at an acceptable risk level. Over the life of the system, many changes occur that may reduce the effectiveness of internal security controls. Security controls typically become outdated and less effective as threats and vulnerabilities evolve. The objective of the System Re-Certification is to ensure that system certification is an on-going process, and that information security is managed throughout the life of the system.	M												
System Re-Accreditation	System Re-Accreditation is the official management decision to authorize continued operation of an information system after acceptable System Re-Certification and any necessary adjustments have been completed.	M												
Disposition Review	A Disposition Review is conducted to ensure that a system/application or other IT situation has been completely and appropriately disposed, thereby ending the lifecycle of the IT investment.	CM												
Independent Verification & Validation (IV&V) Assessment	An IV&V Assessment is conducted by an independent third party to identify potential improvements that may not be apparent to those working directly on a project, or identify problems before they occur and thus avoid loss and minimize the cost of any necessary corrective action. IV&V Assessment also provides management with an independent perspective on the full scope of project activities, from planning through implementation.	CM												
Integrated Baseline Review (IBR)	The IBR is an internal inspection led by the project management team to verify that the project baseline is in place, together with a realistic budget to accomplish all planned work. The IBR includes an evaluation of the performance measurement baseline for realism and inherent risks. When contractor resources are involved, the IBR provides a forum through which the government's team gains a sense of ownership and understanding of the contractor's management process and assurance that earned value management has been appropriately established for the project.	CM												

* M= Mandatory; CM=Conditionally Mandatory