Investment Selection Review (ISR)

Summary Description:

The purpose of the Investment Selection Review (ISR) is for the CMS Information Technology Investment Review Board (ITIRB) to evaluate a proposed IT investment/project to determine if it is a sound, viable investment worthy of funding, support and inclusion in CMS' IT Investment Portfolio.

Status:

Mandatory - The Investment Selection Review (ISR) is the first of three critical checkpoints in the CMS Integrated IT Investment & System Life Cycle Framework. All proposed IT investments/projects must pass an ISR in order to receive funding or further support as a viable CMS IT investment/project.

Timeframe:

The Investment Selection Review (ISR) is initially performed at the end of the IT Investment Selection Phase of the IT investment life cycle and/or at the end of the Business Case Analysis Phase of the system life cycle for all new system development projects and any automated systems undergoing new major architectural design or functional changes. The ISR is also conducted on an annual basis for all new and ongoing IT investments/projects as part of the annual CMS budget/funding process.

Responsible Reviewing Component:

OIS/PMSG has the primary decision authority over the need for an Investment Selection Review (ISR) and primary responsibility for ensuring that the ISR is appropriately conducted.

Primary Information Exchange Partners:

The following are the primary stakeholders who participate in or have an interest in the outcome of the Investment Selection Review (ISR):

Project Owner/Manager
Business Owner(s)/Partner(s)
Component Lead
OIS/ITAPS
OIS/PMSG
OIS/ISMG
Executive Steering Committee (ESC)
CMS Information Technology Investment Review Board (ITIRB)
Chief Information Officer (CIO)
Chief Technology Officer (CTO)

Government Responsibilities:

The Project Owner/Manager works with their designated Component Lead to ensure completion of the entrance requirements for the Investment Selection Review (ISR). The Component Lead collaborates with OIS/PMSG in determining readiness for the ISR. The Project Owner/Manager and Component Lead are responsible for ensuring that all actions resulting from the ISR are satisfactorily completed. The Component Lead is responsible for tracking all critical issues to closure, while the Project Owner/Manager is responsible for tracking and resolution of all other actions resulting from the ISR.

Contractor Responsibilities:

Not Applicable

Entrance Criteria/Inputs:

The following artifacts are mandatory prerequisites to the Investment Selection Review (ISR):

- IT Fact Sheet
- Business Case Analysis (BCA)

A separate Concept of Operations (ConOps) document may also be a prerequisite to the ISR, if deemed appropriate or necessary.

Prior to the ISR, OIS/PMSG should also have evaluated the following:

- System development methodology prescribed for the IT project
- Framework artifacts and reviews prescribed for the IT project
- Proposed acquisition strategy, if applicable
- Qualifications of the designated Project Owner/Manager

Exit Criteria/Outputs:

There are four key questions that must be answered in the affirmative for a proposed IT investment/project to be considered acceptable for funding and further support by CMS:

1. Is the proposed IT investment/project aligned with strategic CMS business objectives and priorities?
2. After analyzing the projected costs and benefits, is a positive return anticipated for the proposed IT investment/project?
3. Is there an acceptable level of risk, and has an appropriate risk mitigation strategy been established for the proposed IT investment/project?
4. Is the technical strategy for the proposed IT investment/project acceptable, and is it compliant with CMS' Enterprise Architecture?

Guidance:

For information regarding CMS' current annual budget/funding process, see: How do I get funding for my IT project?

For additional information or guidance regarding the Investment Selection Review (ISR), contact your designated Component Lead who will put you in touch with a representative from OIS/PMSG to assist you.

Review Process:

The specific process for conducting an Investment Selection Review (ISR) is currently being established by the CMS Information Technology Investment Review Board (ITIRB) and OIS/PMSG and will be described here when that information becomes available.

Date Created/Modified:

March 2005/May 2005

Implementation Readiness Review (IRR)

Summary Description:

The purpose of the Implementation Readiness Review (IRR) is to ensure that the information technology (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 CMS test and/or production environments.

Status:

Conditionally Mandatory - All IT solutions or automated systems/applications (new releases or revisions, including GOTS and/or COTS integrations) that will be hosted or reside within the CMS infrastructure must conduct an Implementation Readiness Review (IRR).

Timeframe:

The Implementation Readiness Review (IRR) is performed at the end of the Development Phase of the system life cycle just prior to transitioning the IT solution or automated system/application into the Implementation & Testing Phase.

Responsible Reviewing Component:

OIS/TMG is the CMS component that has primary responsibility for ensuring that an Implementation Readiness Review (IRR) is appropriately conducted.

Primary Information Exchange Partners:

The following are the primary stakeholders who participate in or have an interest in the outcome of the Implementation Readiness Review (IRR):

Project Owner/Manager
System Developer
Component Lead
OIS/EDG
OIS/TMG
IT Infrastructure Implementation Agent or Contractor

Government Responsibilities:

The Project Owner/Manager works with their designated Component Lead to ensure completion of the entrance requirements for the Implementation Readiness Review (IRR). Representatives from the participating stakeholder groups within the Office of

Information Services (OIS) are responsible for reviewing the input documents prior to the IRR and being prepared to present any critical issues during the IRR. The OIS stakeholders are responsible for ensuring that assumptions, constraints, priorities, issues and risks based on their individual areas of subject matter expertise are identified and addressed during the IRR. The Project Owner/Manager and Component Lead are also responsible for ensuring that all actions resulting from the IRR are satisfactorily completed. The Component Lead is responsible for tracking all critical issues to closure, while the Project Owner/Manager is responsible for tracking and resolution of all other actions resulting from the IRR.

Contractor Responsibilities:

The IT Infrastructure Implementation Agent or Contractor is responsible for identifying any critical issues that may prevent an IT solution or automated system/application from being successfully implemented within the CMS infrastructure. The IT Infrastructure Implementation Agent or Contractor is also responsible for identifying any assumptions, constraints, issues, problems, or concerns that need to be addressed in order to successfully complete implementation activities.

Entrance Criteria/Inputs:

Mandatory artifacts that are input to the Implementation Readiness Review (IRR) include the following:

System Design Document (SDD)
Code
Version Description Document (VDD)
Implementation Plan
Test Plan
Initial draft of Operator Manual

Other inputs that may be required, depending on the specific IT project being addressed, include:

Interface Control Document (ICD)
Database Design Document
Data Conversion Plan
Release Plan
Training Plan

An Engineering Task Order or a Work Order will likely be required for the IT Infrastructure Implementation Agent or Contractor to perform implementation activities. A Work Order can be used only for relatively small efforts, which are covered by the base contract. Efforts that require procurement of equipment or software, installation of newly acquired hardware, ongoing maintenance of equipment or software, etc. that are outside the scope of the current contract will require an Engineering Task Order and associated funding. Prior to the IRR, a draft of a proposed Statement of Work (SOW) covering the implementation activities that the IT Infrastructure Implementation Agent or Contractor will be responsible for completing must be provided to OIS/TMG.

All applicable inputs to the IRR for the specific IT project being addressed are to be provided to the IRR participants at least two weeks prior to the scheduled IRR session.

Exit Criteria/Outputs:

The Implementation Plan must be updated to reflect any changes that are deemed necessary as a result of the Implementation Readiness Review (IRR), and should continue to be updated throughout the implementation process. Also, a final Statement of Work (SOW) with a corresponding HHS-393 Form or an appropriate Work Order must be negotiated before the IT Infrastructure Implementation Agent or Contractor can begin any implementation activities.

Guidance:

For information or guidance regarding the Implementation Readiness Review (IRR), contact your designated Component Lead who will put you in touch with a representative from OIS/TMG to assist you.

Review Process:

The specific process for conducting an Implementation Readiness Review (IRR) is currently being established by the Office of Information Services (OIS) and will be described here when that information becomes available.

Date Created/Modified:

March 2002/August 2005

Operational Readiness Review (ORR)

Summary Description:

The purpose of the Operational Readiness Review (ORR) is to conduct a formal inspection to determine if the final information technology (IT) solution or automated system that has been developed, implemented and tested is ready for release into the production environment for sustained operations and maintenance support.

Status:

Mandatory - The Operational Readiness Review (ORR) is the last of three critical checkpoints in the CMS Integrated IT Investment & System Life Cycle Framework. All IT solutions or automated systems/applications (new releases or revisions) must conduct an ORR to ensure that the IT solution or automated system/application (including GOTS and/or COTS integration) that has been developed, implemented and tested is ready for release into the production environment for sustained operations and maintenance support. An ORR is required regardless of whether or not the IT solution or automated system/application is hosted within the CMS Data Center.

Timeframe:

The Operational Readiness Review (ORR) is performed at the end of the Implementation & Testing Phase of the system life cycle just prior to the automated system being released into the production environment for sustained operations and maintenance support during the subsequent Operations & Maintenance Phase.

Responsible Reviewing Component:

OIS/TMG is the CMS component that has primary responsibility for the Operational Readiness Review (ORR) and for ensuring that the final solution or automated system is ready for release into the production environment for sustained operations and maintenance support.

OIS/PMSG has primary responsibility for ensuring that the ORR is appropriately conducted.

Primary Information Exchange Partners:

The following are the primary stakeholders who participate in or have an interest in the outcome of the Operational Readiness Review (ORR):

Project Owner/Manager
System Owner/Manager
Component Lead

OIS/EDG
OIS/ISMG
OIS/ITAPS
OIS/PMSG
OIS/SSG
OIS/TMG
IT Infrastructure Implementation Agent or Contractor
CBC/BISG/DWPM (Internet-facing systems only)
Chief Technology Officer (CTO)
Executive Steering Committee (ESC)
Business Owners/Partners
Configuration (or Change) Control Board (CCB)

Government Responsibilities:

The Project Owner/Manager works with their designated Component Lead to ensure completion of the entrance requirements for the Operational Readiness Review (ORR). Representatives from the participating stakeholder groups are responsible for reviewing the input documents prior to the ORR and being prepared to present any critical issues during the ORR. The participating stakeholders are responsible for ensuring that assumptions, constraints, priorities, issues, and risks based on their individual areas of subject matter expertise are identified and addressed during the ORR. The Project Owner/Manager and Component Lead are also responsible for ensuring that all actions resulting from the ORR are satisfactorily completed. The Component Lead is responsible for tracking all critical issues to closure, while the Project Owner/Manager is responsible for tracking and resolution of all other actions resulting from the ORR.

Contractor Responsibilities:

The IT Infrastructure Implementation Agent or Contractor is responsible for identifying any critical issues that would prevent an IT solution or automated system/application from being released into the production environment for sustained operations and maintenance support. The IT Infrastructure Implementation Agent or Contractor is also responsible for identifying any assumptions, constraints, issues, problems, or concerns that may need to be addressed after production release.

Entrance Criteria/Inputs:

The following artifacts are mandatory prerequisites to the Operational Readiness Review (ORR):

- Version Description Document (VDD)
- Implementation Plan
- Test Summary Report
- Operator Manual
- Signed System Accreditation Form

Other artifacts that may also be prerequisites to the ORR, depending on the specific IT project being addressed, include:

- Final System of Records (SOR)
- Final Computer Match Agreement (CMA)
- Final Data Use Agreement (DUA)
- Training Artifacts
- User Manual

The Version Description Document (VDD), Test Summary Report and Operator Manual are to be provided to the ORR participants at least two weeks prior to the scheduled ORR session.

Exit Criteria/Outputs:

The following are the results/outputs that are to be documented from the Operational Readiness Review (ORR):

1. Assumptions
2. Constraints
3. Issue Resolutions
4. Unresolved Issues
5. Risk Mitigation Strategies
6. Recommendations
7. Action Items

Another output of the ORR is the ORR Exit Form (Word Document) that contains signatures from all of the representatives of the primary stakeholder groups and any documented critical issues they have identified that must be resolved before the IT solution or automated system/application can move into the production environment. If no critical issues are identified by a primary stakeholder group, then the representative's signature indicates concurrence for the IT solution or automated system/application to move into the production environment.

Guidance:

For information or guidance regarding the Operational Readiness Review (ORR), contact your designated Component Lead who will put you in touch with a representative from OIS/TMG to assist you.

Review Process:

The specific process for conducting an Operational Readiness Review (ORR) is currently being established by the Office of Information Services (OIS) and will be described here when that information becomes available.

Date Created/Modified:

March 2005/May 2005

System Certification

Summary Description:

System Certification is the comprehensive evaluation by the System Owner/Manager of the management, operational, and technical security controls implemented for an information system to ensure compliance with CMS' information security requirements. The certification evaluation includes review of the Information Security (IS) Risk Assessment (RA), System Security Plan (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 within the ST&E report and delivered to the System Owner/Manager for corrective action 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) by the System Owner/Manager. A System Certification Package, which includes the appropriate Certification Form(s), IS RA, SSP (if applicable), and ST&E report is submitted to OIS/SSG for subsequent System Accreditation (i.e., authorization to process) by the CMS Chief Information Officer (CIO) / Designated Approval Authority (DAA).

Status:

Mandatory - All CMS information systems must complete an initial System Certification within the CMS business component before the System Security Plan (SSP) and/or Information Security (IS) Risk Assessment (RA) can be forwarded for initial System Accreditation.

Timeframe:

System Certification is initiated and completed during the Implementation & Testing Phase and must be performed before System Accreditation.

Responsible Reviewing Component:

OIS/SSG is the CMS component that has the primary responsibility for ensuring that System Certification is appropriately conducted in accordance with the CMS System Security Plan (SSP) Methodology and/or the Information Security (IS) Risk Assessment (RA) Methodology, as well as in accordance with the CMS Information Security Certification and Accreditation (C&A) Methodology and the CMS Information Security

Certification and Accreditation (C&A) Procedure. OIS/SSG is also responsible for ensuring that the SSP Certification Form and/or IS RA Certification Form for initial or interim certification of the SSP and/or IS RA are appropriately completed and signed.

Primary Information Exchange Partners:

The following are the primary stakeholders who participate in the System Certification or have an interest in the outcome:

Project Owner/Manager
System Owner/Manager
System Maintainer (Manager)
Component Information Systems Security Officer (ISSO)
Certification & Accreditation (C&A) Evaluator
OIS/SSG

Government Responsibilities:

The Component Information Systems Security Officer (ISSO), System Owner/Manager and System Maintainer (Manager) must examine the controls implemented for the information system and attest to the successful completion of the appropriate technical certification evaluations. This ensures that the inherent risk in processing on a network or at the installation(s) that support the system, particularly where the support system is operated outside of CMS management control, is understood and accepted by the System Owner/Manager and System Maintainer (Manager). The Component ISSO, System Owner/Manager and System Maintainer (Manager) must complete and sign the System Security Plan (SSP) Certification Form and/or Information Security (IS) Risk Assessment (RA) Certification Form. The Certification Restrictions page of the Certification Form(s) must state any restrictions on use of the system that are being self-imposed by the System Owner/Manager. If the System Owner/Manager is not satisfied that the system is protected at an acceptable level of risk, a certification can be granted allowing time for implementation of additional controls. The Certification Actions page of the Certification Form(s) is completed by the System Owner/Manager to list all of the planned enhanced controls to address identified vulnerabilities to the system and the anticipated completion dates.

Upon completion of System Certification, it is the responsibility of the System Owner/Manager to submit a complete System Certification Package to OIS/SSG for subsequent System Accreditation. The System Certification Package must contain:

- Completed Certification Form(s) signed by all relevant parties.
- System Accreditation Form with the name of the system and the name of the CMS component and System Owner/Manager responsible for the system identified.
- Completed SSP and/or IS RA, including all relevant appendices and attachments.

- Any relevant documentation produced during security assessments, reviews, audits, technical testing and analysis (e.g., ST&E report), if applicable.

Contractor Responsibilities:

An independent contractor (i.e., Certification & Accreditation (C&A) Evaluator) may be utilized to examine the controls implemented for the information system and to attest to the successful completion of the appropriate technical certification evaluations for designated General Support Systems (GSSs) and Major Applications (MAs).

Entrance Criteria/Inputs:

Mandatory artifacts that are input to the System Certification include the following:
System Security Plan (SSP) and/or Information Security (IS) Risk Assessment (RA)

Exit Criteria/Outputs:

A System Certification Package must be prepared, which contains the following items:

- Completed/Signed System Security Plan (SSP) Certification Form and/or Information Security (IS) Risk Assessment (RA) Certification Form
- System Accreditation Form with the name of the system and the name of the CMS component and System Owner/Manager responsible for the system identified.
- Completed System Security Plan (SSP) and/or Information Security ((S) Risk Assessment (RA), including all relevant appendices and attachments.
- Any relevant documentation produced during security assessments, reviews, audits, technical testing and analysis (e.g., ST&E report), if applicable.

A hardcopy of the complete System Certification Package, as well as a softcopy, are to be delivered to OIS/SSG (mailstop: N2-14-26, telephone: 410-786-0953) for subsequent System Accreditation at least 60 days prior to the system going into production.

Guidance:

Information and guidance regarding System Certification can be obtained from within the following documents:

System Security Plan (SSP) Methodology (PDF - 354KB)
Information Security (IS) Risk Assessment (RA) Methodology (PDF - 281KB)
CMS Information Security Certification and Accreditation (C&A) Methodology (PDF - 600KB)
CMS Information Security Certification and Accreditation (C&A) Procedure (PDF - 712KB)

For additional guidance regarding System Certification, contact OIS/SSG.

Review Process:

The Project Owner/Manager forwards a blank System Security Plan (SSP) Certification Form and/or Information Security (IS) Risk Assessment (RA) Certification Form along with the baselined SSP and/or IS RA for the information system to the Component Information Systems Security Officer (ISSO), System Owner/Manager and System Maintainer (Manager) for review and technical certification evaluation. For designated General Support Systems (GSSs) and Major Applications (MAs), an independent contractor (Certification & Accreditation (C&A) Evaluator) may be utilized to also examine the controls implemented for the information system and to attest to the successful completion of the appropriate technical certification evaluations. The results of the certification assessment, together with a review of any other independent audits, reviews or assessments are documented within the ST&E report and delivered to the System Owner/Manager for corrective action 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) by the System Owner/Manager.

The Component ISSO, System Owner/Manager and System Maintainer (Manager) complete and sign the SSP Certification Form and/or IS RA Certification Form. The Certification Restrictions page of the Certification Form(s) must state any restrictions on use of the system that are being self-imposed by the System Owner/Manager. If the System Owner/Manager is not satisfied that the system is protected at an acceptable level of risk, a certification can be granted allowing time for implementation of additional controls. The Certification Actions page of the Certification Form(s) is completed by the System Owner/Manager to list all of the planned enhanced controls to address identified vulnerabilities to the system and the anticipated completion dates. A hardcopy of the complete System Certification Package, as well as a softcopy, are to be delivered to OIS/SSG (mailstop: N2-14-26, telephone: 410-786-0953) for System Accreditation at least 60 days prior to the system going into production.

Date Created/Modified:

March 2002/March 2005

System Accreditation

Summary Description:

System Accreditation is CMS' 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 System Security Plan (SSP) and/or Information Security (IS) Risk Assessment (RA). Ultimately, the CIO/DAA must strike a firm balance between authorizing the operation of information systems necessary to support completion of the CMS business mission, while ensuring that an adequate level of information security is in place. CMS must strive to implement the most effective security controls, in consideration of technical, budgetary, time, and resource limitations, while continuing to support business mission requirements.

Status:

Mandatory - All CMS information systems must complete an initial or interim System Accreditation prior to the information system being released into production for sustained operations and maintenance support. An initial System Accreditation granting approval to operate will not exceed three years, after which System Re-Certification and System Re-Accreditation must occur. If the system is not initially protected at an acceptable level of risk, an interim System Accreditation may be granted in lieu of a full denial to process allowing time for implementation of additional security controls. An interim System Accreditation may be granted for a fixed period of time, not to exceed one year, while continuing the management authorization process thereby permitting the system to meet its operational business requirements until its information security posture is improved.

Timeframe:

System Accreditation is initiated and completed during the Implementation & Testing Phase only after System Certification has been completed for the information system and prior to the Operational Readiness Review that is required before the system is moved into production for sustained operations and maintenance support during the Operations & Maintenance Phase.

Responsible Reviewing Component:

OIS/SSG is the CMS component that has the primary responsibility for ensuring that System Accreditation is appropriately conducted in accordance with the CMS System Security Plan (SSP) Methodology and/or the Information Security (IS) Risk Assessment (RA) Methodology, as well as in accordance with the CMS Information Security Certification and Accreditation (C&A) Methodology and the CMS Information Security Certification and Accreditation (C&A) Procedure. OIS/SSG is also responsible for ensuring that the System Accreditation Form for initial or interim accreditation is appropriately completed and signed.

Primary Information Exchange Partners:

The following are the primary stakeholders who participate in the System Accreditation or have an interest in the outcome:

Project Owner/Manager
System Owner/Manager
System Maintainer (Manager)
Component Information Systems Security Officer (ISSO)
Chief Technology Officer (CTO)
Chief Information Officer (CIO)
OIS/SSG

Government Responsibilities:

The System Owner/Manager must ensure that the information and resources necessary to make an informed decision on whether to authorize operation of an information system are available to the Chief Information Officer (CIO) / Designated Approval Authority (DAA). At this time CMS has not assigned a DAA; therefore, only the CIO is authorized to accredit CMS systems. The CMS CIO and the Chief Technology Officer (CTO) examine the signed Information Security (IS) Risk Assessment (RA) Certification Form, the System Security Plan (SSP) Certification Form (if applicable), the IS RA and SSP (if applicable) for the information system to determine if a satisfactory level of operational security risk has been established for the system. The CMS CIO/DAA signs the System Accreditation Form indicating approval or denial of system accreditation based on any restrictions or specific actions designated in Attachments B and C of the form. The signature of the CMS CIO/DAA further attests that the controls implemented for the system have been examined and are adequate to meet CMS IS policies and standards and that the system appears to be operating at an acceptable level or risk. The Project Owner/Manager, System Owner/Manager, System Maintainer (Manager), and Component Information Systems Security Officer (ISSO) all have an interest in the outcome of the System Accreditation.

Contractor Responsibilities:

Not Applicable

Entrance Criteria/Inputs:

A System Certification Package, which contains the following items, must be provided for System Accreditation:

- Completed/Signed System Security Plan (SSP) Certification Form and/or Information Security (IS) Risk Assessment (RA) Certification Form
- System Accreditation Form with the name of the system and the name of the CMS component and System Owner/Manager responsible for the system identified
- Completed System Security Plan (SSP) and/or Information Security (IS) Risk Assessment (RA) including all relevant appendices and attachments.
- Any relevant documentation produced during security assessments, reviews, audits, technical testing and analysis (e.g., ST&E report) if applicable.

Exit Criteria/Outputs:

Mandatory artifacts that are output from the System Accreditation, which serve as input to the subsequent Operational Readiness Review (ORR), include the following:

Completed/Signed System Accreditation Form

Guidance:

Information and guidance regarding System Accreditation can be obtained from within the following documents:

System Security Plan (SSP) Methodology (PDF - 354KB)
Information Security (IS) Risk Assessment (RA) Methodology (PDF - 281KB)
CMS Information Security Certification and Accreditation (C&A) Methodology (PDF - 600KB)
CMS Information Security Certification and Accreditation (C&A) Procedure (PDF - 712KB)

For additional guidance regarding System Accreditation, contact OIS/SSG.

Review Process:

OIS/SSG forwards the System Accreditation Form, the signed System Security Plan (SSP) Certification Form and/or Information Security (IS) Risk Assessment (RA) Certification Form, and the SSP and/or IS RA for the information system, provided in the

System Certification Package to the CMS Chief Information Officer (CIO) and the Chief Technology Officer (CTO). The CMS CIO and CTO review the SSP and/or IS RA and the associated certification form(s) for the information system and determine if a satisfactory level of operational security risk has been established for the system. Depending on the complexity and criticality of the system, the CIO and CTO may request a briefing by the System Owner/Manager on the information system, the business functions it supports and the security controls that minimize the security risk. The CMS CIO signs the System Accreditation Form indicating approval or denial of system accreditation based on any restrictions or specific actions designated in Attachments B and C of the form. The signature of the CMS CIO further attests that the controls implemented for the system have been examined and are adequate to meet CMS information security policies and standards and that the system appears to be operating at an acceptable or unacceptable level of risk. System Accreditation will not exceed three years.

Conditional management approval to process can be granted for a fixed period of time, not to exceed one year. This authority is based on an approved SSP and/or IS RA System Certification, and is contingent on certain conditions being met. The interim approval to operate, while continuing the management authorization process, permits the system to meet its operational business requirements while improving its information security posture. If the CMS CIO is not satisfied that the system is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. Interim approval can only be granted by the CMS CIO in lieu of a full denial to process and for no more than one year. Interim approval to operate is not a waiver of the requirement for management approval to process. The information system must meet all requirements and receive management approval to process by the interim approval expiration date. No extensions of interim accreditation can be granted except by the CMS CIO.

Date Created/Modified:

March 2002/March 2005