HHS Enterprise Performance lifecycle (EPLC) Framework

Role of Critical Partners
Information Security

Version *0.5*

December 2009

This Final Draft Critical Partner Guidance Manual is based upon
HHS Enterprise Performance Life Cycle Framework dated January 18, 2010
Pending CDC IR Governance Approval

TABLE OF CONTENTS

Summary

EPLC Background

In October 2008, HHS issued the HHS OCIO Policy for Information Technology (IT) Enterprise Performance Life Cycle (EPLC) along with the EPLC Framework. The EPLC framework consists of ten life cycle phases. Within each phase, activities, responsibilities, reviews, and deliverables are defined. Exit criteria are established for each phase and Stage Gate reviews are conducted through the IT governance process to ensure that the project's management quality, soundness, and technical feasibility remain adequate and the project is ready to move forward to the next phase. The EPLC framework provides a guide to Project Managers, Business Owners, IT Governance Executives, other Stakeholders, and Critical Partners throughout the life of the project.

The EPLC framework is designed to provide the flexibility needed to adequately manage risk while allowing for differences in project size, complexity, scope, duration, etc. Examples of flexibility include the ability (with IT governance approval) to tailor the framework where particular phases or deliverables may not apply, to aggregate phases and deliverables when appropriate, to provide for conditional stage gate approvals that allow progress to a subsequent phase in a manner that identifies and controls for risk.

The EPLC is a framework for managing the life cycle for **projects**. It recognizes that there is an implied hierarchy of an IT portfolio made up of IT investments, which are made up of projects, which are made up of systems. When a project has only one system, or an investment has only one project, then the distinction of exactly what is a project can become blurred. In CDC, investments are comprised of one or more projects and include those covered both by development/modernization/enhancement funding and by steady state funding for ongoing operations and maintenance. Each project within the investment is required to follow the EPLC. The annual Capital Planning & Investment Control (CPIC) process will address the investment as an entity and will ensure that each project within the investment has been compliant with the requirements.

Small Projects

Although the first glance of this manual will give the impression of too much "overhead" for small projects, Critical Partners are encouraged to work with the Project Managers and Business Owners to identify the amount of rigor required for success. Many of the project deliverables and reviews can be tailored (i.e., used, not used, or combined) to fit the needs of a small project using the standard EPLC Project Process Agreement template; however, for consistency, this manual is inclusive of all requirements without tailoring. CDC is currently working on defining a Project Process Agreement for small and fast-track projects which will provide more detailed guidance. It is expected that this document will be available in February 2010.

Purpose of this Manual

The purpose of this manual is to abstract out the relevant requirements for the Information Security Critical Partner within the EPLC and CDC's implementation of the requirements. This manual is intended to be used as a quick reference manual.

Role of a Critical Partner in a Project

Overview

The EPLC framework and associated best practices in IT project management combine to reduce risk within individual IT projects and across the HHS and CDC IT investment portfolio. Only sound, viable IT projects with reasonable baselines for funding should be included in the IT investment portfolio. EPLC requires that IT projects be managed and implemented in a structured manner, using sound project management practices, and involving business stakeholders and technical experts throughout the project's life cycle.

Critical Partners are essential project stakeholders. EPLC defines Critical Partners as functional managers in nine areas: Enterprise Architecture (EA), Security, Acquisition Management, Finance, Budget, Human Resources, Section 508, Capital Planning and Investment Control (CPIC), and Performance (the Business Owner). They participate in IT projects and governance decisions to confirm compliance with policies in their respective areas and to make timely tradeoff decisions where conflicts arise during the planning and execution of projects. National Centers at CDC may also define other Critical Partner roles such as Health Scientists, Statisticians, or Epidemiologists. In this document the term National Center encompasses all organizational entities at CDC including Offices and Institutes. Because organizational structures vary at CDC, the expertise for these Critical Partner roles may be fulfilled in various ways as defined by the National Centers; however, the general guidance of the roles as defined below should be considered in the National Center definitions.

Overall Responsibility for each Critical Partner

Enterprise Architecture

The EA Critical Partners are charged with ensuring that the CDC Enterprise Architecture Program supports, augments, and reinforces the EPLC process to ensure achievement of the mission, strategic and operational business needs of CDC. Their goal is to ensure that an IT project provides demonstrable alignment with CDC architecture principles, business processes, and technical architecture.

Security

The Security Critical Partners are charged with ensuring that the CDC Security Program supports, augments, and reinforces the EPLC process to ensure achievement of the mission, strategic and operational business needs of CDC. They must ensure that all projects demonstrate that the appropriate planning and budgeting for the appropriate IT privacy and security controls are explicitly incorporated into the life cycle.

Acquisition Management

The Acquisition Management Critical Partners are charged with ensuring that the CDC Procurement and Grants Office supports, augments, and reinforces the EPLC process to ensure achievement of the mission, strategic and operational business needs of CDC. They are responsible for reviewing project business cases for conformance with the Federal Acquisition Regulation, HHS Department and CDC acquisition policies and procedures, and successful business practices.

Finance & Budget

CDC has combined the responsibilities of the Budget and Finance Critical Partners into a single Critical Partner role and has prepared one manual to address both areas. The Finance & Budget Critical Partners are responsible for ensuring that the business case and project's financial needs are adequately identified and planned and that any of the project's financial management components interact with financial systems in such a way as to ensure compliance with financial and budget standards and regulations. During the lifecycle of the project, the Finance & Budget Critical Partners provide guidance to project managers regarding financial management and budget policies and issues.

Human Resources/Business Owner

The Human Resources Critical Partners are responsible for ensuring that the project has the skills and competencies necessary to accomplish the business objectives and that all human resource and union issues that may affect a project's progress are addressed in an appropriate manner. The Atlanta Human Resources Center (AHRC) handles HR issues for Civil Service personnel while HR issues for Commissioned Corps personnel is handed by the Office of Workforce and Career Development (OWCD). All training is handled by OWCD. The Business Owner of a project is most often responsible for ensuring that the project has the skills and competencies required; therefore, a combination of individuals may need to fulfill this responsibility.

Section 508

The Section 508 Critical Partners are responsible for reviewing the IT business cases and project deliverables to ensure that the project design and any associated contracts contain all of the accessibility requirements and those issues are identified and addressed prior to implementation.

CPIC

The CPIC Critical Partners are responsible for reviewing IT business cases and project deliverables to ensure compliance with CPIC policies and procedures and for providing guidance to IT project managers regarding the overall project management requirements of EPLC and CPIC. They are also responsible for the coordination of the other Critical Partners in the preparation and review during Stage Gates.

Performance/Business Owner

The Performance Critical Partners are the Business Owners who are responsible for ensuring that their projects achieve the mission, strategic and operational business needs of CDC while meeting the business need as originally identified. The Business Owner are responsible for identifying the business needs and the performance measures to be satisfied by their projects and have the overall financial and management responsibility.

EPLC Framework

The EPLC framework shown in Figure 1 consists of ten life-cycle phases and three major lanes of activities that are conducted during a phase. Critical Partners have responsibilities in all phases and lanes of activities. This manual provides specific information for the Information Security Critical Partner on all responsibilities.

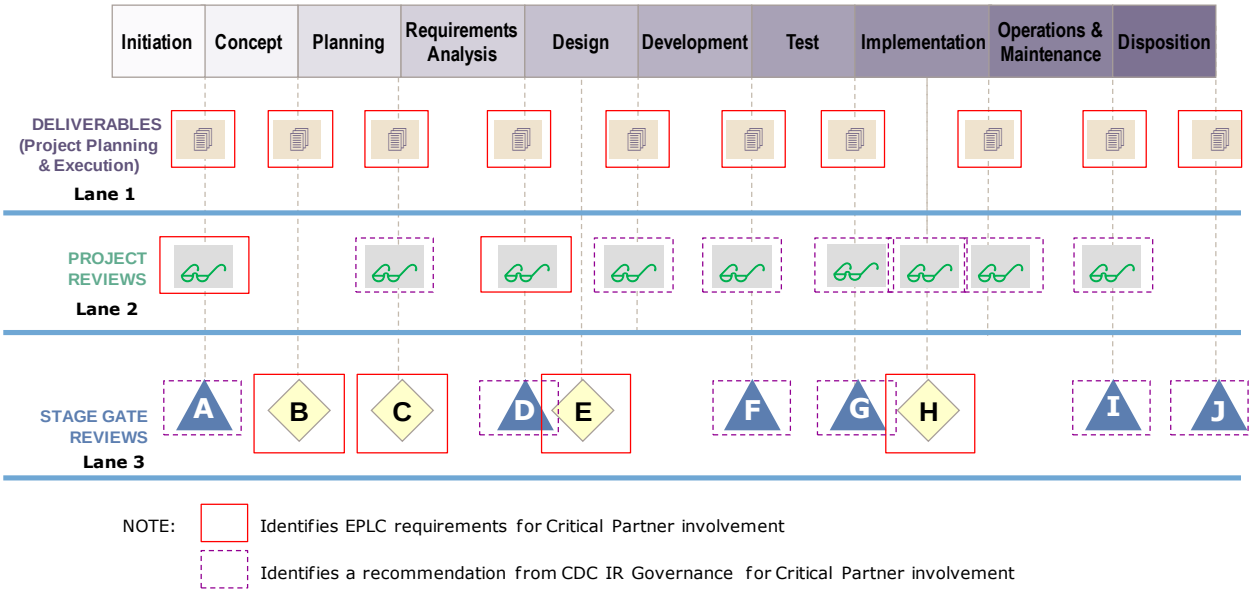

Figure 1. EPLC Framework Showing Phases and Three Lanes of Activities

Lane 1: Deliverables (Project Planning & Execution)

The project manager is responsible and accountable to the Business Owner for meeting the business requirements of a project within the cost, schedule, and scope baselines. In order for a project manager to be successful, **Critical Partners need to ensure that project requirements from their respective areas are planned for at the earliest possible point in the project**. This requires that Critical Partners be **actively engaged** in the project from beginning to end. EPLC also considers Critical Partners to be members of the Integrated Project Team assisting project managers with the planning and execution of the project.

Lane 2: Project Reviews

There are 13 different project reviews that are required by the EPLC. These project reviews are conducted at specific points in the life cycle to confirm that events have occurred and decisions have been made before continuing with the project. Some of these reviews may be performed concurrently, e.g., the System Re-Certification and System Re-Accreditation Project Reviews in EPLC will be performed as a part of the CDC Certification & Accreditation process. The different project reviews are spelled out in the individual phases with indication of the requirements for the Critical Partners.

The EPLC requires Critical Partner participation in the Architecture Review [Initiation Phase] and Requirements Review [Requirements Analysis Phase]. National Centers may also require Critical Partner

participation in some or all of the remaining project reviews as a method for Critical Partners to provide oversight, advice and counsel to the project manager on a regular basis.

CDC is in the process of developing additional information and guidance on conducting project reviews including specific information for each review.

Lane 3: Stage Gate Reviews

Stage Gate Reviews are conducted by CDC IR Governance as defined in the CDC IR Governance Stage Gate Review Plan. In this plan, CDC IR Governance has defined a process for the IR Governance bodies to conduct the following four Stage Gates:

- Project Selection Review [B]
- Project Baseline Review [C]
- Preliminary Design Review [E]
- Operational Readiness Review [H]

For these four gates, each Critical Partner will be responsible for reviewing projects to ensure that the project meets Critical Partners' respective requirements. Based on these reviews, Critical Partners must provide recommendations to the applicable IR Governance bodies on whether the project should proceed to the next phase [with or without condition] or whether the project should be discontinued. The CPIC Critical Partner is responsible for coordinating these Critical Partner reviews.

The IR Governance Stage Gate Review Plan requires that projects with an annual budget of $1 million or greater be reviewed at the CDC Enterprise level. For projects with an annual budget of less than $1 million, the National Center Governance body is responsible.

The National Center Governance body also has the responsibility for determining the most appropriate approach for conducting the following Stage Gate Reviews, irrespective of the projects' annual budget:

- Initiation Phase End Stage Gate Review [A]
- Requirements Analysis Phase End Stage Gate Review[D]
- Development Phase End Stage Gate Review [F]
- Test Phase End Stage Gate Review [G]
- Operations & Maintenance Phase End Stage Gate Review [I]
- Disposition Phase End Stage Gate Review [J]

These gates may be delegated to individuals or organizations inside the Center or performed by the National Center Governance. The role of Critical Partners in these reviews will vary based on the decisions of the National Center's governance body. This manual provides information and guidance to the Information Security Critical Partner for all ten Stage Gate Reviews in case they are called upon for providing a recommendation.

The following graphic in Figure 2 represents the high level process that CDC has utilized in our definition of CDC's Stage Gate Review processes. **Critical Partners in conjunction with the Project Manager, Business Owner and IR Governance bodies must remember that the degree of rigor applied to each Stage Gate Review needs to reflect a consideration of the size of the project, level of technical risk, complexity, and criticality to the CDC mission.**

No project should proceed into the next phase without receiving a decision to proceed for the IR Governance Review body or delegated authority.

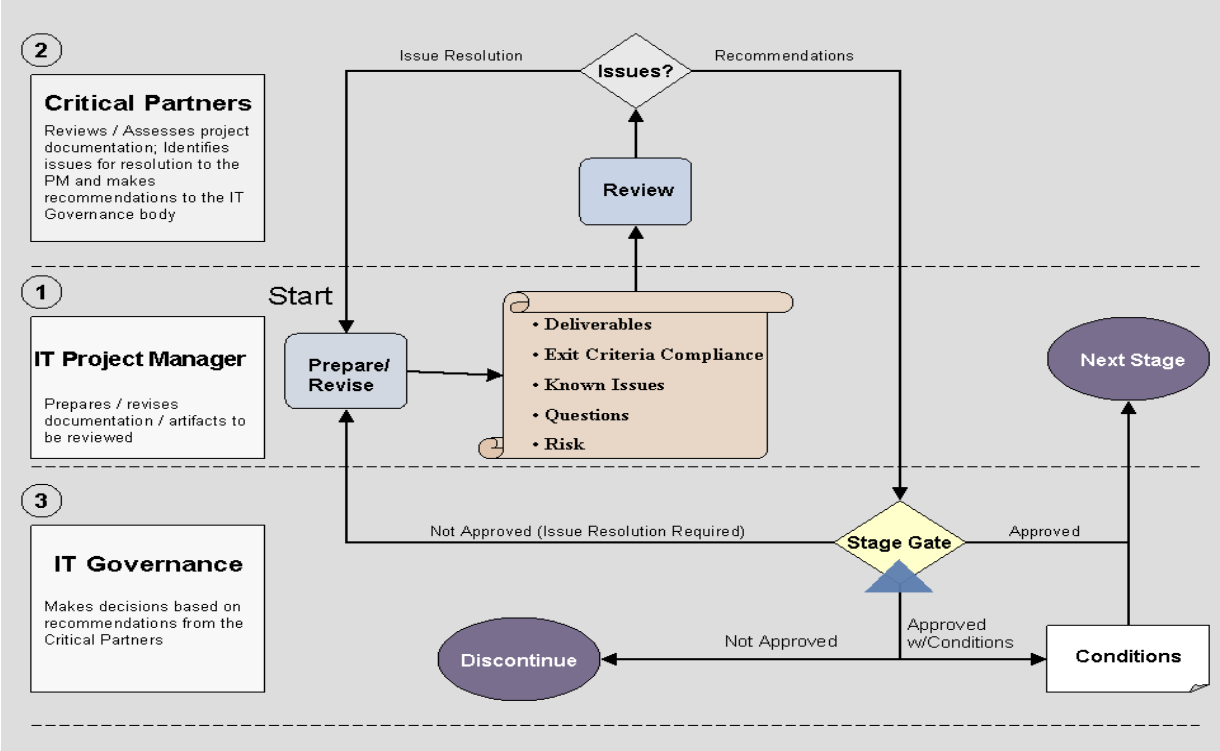

Figure 2. CDC Stage Gate Review Process

Probing Questions

Probing Questions are provided to help Critical Partners know what to ask as a part of their responsibilities in all three lanes of project activities. These questions have been separated into Major Probing Questions and Additional Questions. The major probing questions are those that have been identified as providing significant information for the phase activities. The additional questions should also be considered as appropriate for the size of the project, level of technical risk, complexity, and criticality to the CDC mission. While the Major Probing Questions are included in the sections with responsibilities by phase, additional questions are located in the following section of this manual Additional Questions.

Summary

Critical Partners are key project stakeholders and must be involved in all phases and activities of a project including the project planning and execution along with the appropriate reviews that occur throughout the life cycle. This manual serves as one available resource that may be helpful in accomplishing the required responsibilities of the Information Security Critical Partner. Other resources available to CDC Critical Partners are identified in the Resources Section of this manual.

Role of an Information Security Critical Partner in Initiation Phase

Brief Description of Phase

The Initiation phase identifies the business need, Rough Order of Magnitude (ROM) cost and schedule, and basic business and technical risks. The outcome of the Initiation Phase is the decision to invest in a full business case analysis and preliminary project management plan.

Information Security Responsibilities

Deliverables (Project Planning & Execution) Lane 1	❖ Review the Business Needs Statement. ❖ Determine if the Business Need Statement contains any potential information security concerns.
Project Reviews Lane 2	❖ Participate in the Architecture Review as appropriate to your subject matter expertise to determine if Business Needs Statement is sound and consistent with Enterprise Architecture ▪ Architecture Review purpose is to ask the questions: 1. Does the project potentially duplicate, interfere or contradict another project? 2. Can the project leverage another project (investment) effort? 3. Does this other project already exist? 4. Is another project already proposed, under development or planned for near-term disposition?
Stage Gate Reviews Lane 3	❖ Participate in the Initiation Stage Gate Review if requested by the National Center's IR Governance Plan and as appropriate to your subject matter expertise by providing a recommendation on the following Stage Gate Review questions: 1. Does the Business Needs Statement justify proceeding to the development of a full Business Case and preliminary Project Management Plan, based on the following? • A business owner has been identified and confirmed • Approval of the project is highly probable • Project description is sufficient to permit development of an acceptable business case and preliminary project management plan 2. Are the plans for the development of a business case and preliminary Project Management Plan realistic and achievable with the available resources?
Major Probing Questions for the Information Security Critical Partner	❖ Use the following questions to assist you with completing your responsibilities for this phase as appropriate to your subject matter expertise. Additional questions are located in the Additional Questions section of this manual. 1. What are the potential information security concerns that are raised

	by the project? 2. What, if any, issues and/or risks from your perspective do you see that would affect the development of a business case? 3. How does the proposed project compare to the existing CDC Enterprise Architecture transition plan or to the initiatives that support the CDC IT Strategic Plan's goals and objectives?

Role of an Information Security Critical Partner in Concept Phase

Brief Description of Phase

The Concept phase identifies the high level business and functional requirements required to develop the full business case analysis and preliminary Project Management Plan for the proposed project. The outcomes of the Concept Phase are selection of the project to the CDC IT investment portfolio; approval of initial project cost, schedule and performance baselines; and issuance of a Project Charter.

Information Security Responsibilities

Deliverables (Project Planning & Execution) Lane 1	❖ Review and comment on the Business Case. ❖ Conclude that all applicable information security and privacy standards have been considered in sufficient detail as part of the Business Case. ❖ Verify that 1. the Project has been categorized correctly under FIPS 199 and NIST guidelines; 2. a System Accreditation Memorandum has been correctly initiated; 3. an Electronic Authentication Risk Assessment has been correctly performed in compliance with OMB and NIST guidelines; 4. a Privacy Threshold Analysis has been correctly performed so as to determine if a full PIA will be required to support the Project; 5. the Minimum Baseline Security Requirements (MBLSR) have been selected correctly from the NIST Security Controls Catalog; 6. the Initial Security Risk Assessment Report has been completed in accordance with NIST guidelines.

Project Reviews Lane 2	Note: There are no formal project reviews required during the Concept Phase

Stage Gate Reviews Lane 3	❖ Participate in the Project Selection Stage Gate Review as appropriate to your subject matter expertise by providing a recommendation on the following Stage Gate Review questions: 1. Does the Business Case contain a scope that will meet the high level business requirements? 2. Are the project organizational structure and competencies of the team sufficient to support the project and project manager? 3. Does the Project Charter adequately authorize the project to proceed based on the agreed upon project scope? 4. Does the Preliminary Project Management Plan adequately define how the project will be executed, monitored and controlled and include high level cost and schedule estimates? 5. Does the high level analysis demonstrate that the outcomes will be aligned with the CDC Target Enterprise Architecture? 6. Has the Business Case considered all applicable information security and privacy standards in sufficient detail including FIPS-199 categorization and the initial assessment of the system accreditation

	boundaries? 7. Has a Designated Approving Authority (DAA) been identified? 8. Are the plans for the planning and subsequent phases realistic and achievable with the available resources?

Major Probing Questions for the Information Security Critical Partner	❖ Use the following questions to assist you with completing your responsibilities for this phase as appropriate to your subject matter expertise. Additional questions are located in the Additional Questions section of this manual. 1. How have the applicable information security and privacy standards been addressed in the Business Case, and how was the project categorized according to FIPS-199? 2. How has the threat environment in which the system will operate been covered in the high level information security analysis and preliminary risk assessment? 3. Has an alternatives analysis been done? Are the conclusions reasonable? 4. Have the applicable information security and privacy standards been considered as a part of the business case? 5. What issues and/or risks do you see that would affect the continuation of the project into the planning phase and subsequent requirements analysis, design, development, testing & implementation?

Role of an Information Security Critical Partner in Planning Phase

Brief Description of Phase

The Planning phase completes the development of the full Project Management Plan – and refinement of project cost, schedule and performance baselines as necessary. Outcome of the Planning phase is complete and adequate project planning and sufficient requirements determination to validate the planning and project baselines.

Information Security Responsibilities

Deliverables (Project Planning & Execution) Lane 1	❖ Assess completeness of Planning Phase activities. ❖ Assess robustness of the plan for the Requirement Analysis and subsequent phases. ❖ Assess the availability of resources to execute the Requirement Analysis and subsequent phases. ❖ Ensure the PMP Risk Management Plan accurately establishes that information security and privacy requirements have been identified and planned for. ❖ Ensure that the System Categorization, MBLSR, Initial System Security Plan, Risk Assessment, and preliminary IT Contingency Plans are reviewed and ready for approval by the DAA.

Project Reviews Lane 2	❖ Participate in the Integrated Baseline Review as appropriate to your subject matter expertise if requested by the National Center's IR Governance Plan or by the Project Manager ▪ Integrated Baseline Review purpose is to: 1. Validate that the project baseline and a realistic budget exist to accomplish all planned work 2. Evaluate Performance Measurement Baseline for realism and inherent risks 3. Validate that contractor's management process and ensures that earned value management practices are in place

Stage Gate Reviews Lane 3	❖ Participate in the Project Baseline Stage Gate Review as appropriate to your subject matter expertise by providing a recommendation on the following Stage Gate Review questions: 1. Does the Business Case contain a full scope of the project that will meet the business need if the high level requirements are met? 2. Is the Project Management Plan (including all of the components and recommendations for cost, schedule, and scope baselines) fully scaled to meet the needs of a successful project? 3. Have all deliverables been defined and an acceptable Project Process Agreement utilized to justify modifications to the EPLC framework if needed? 4. Has the Acquisition Strategy including all applicable contract clauses

	been approved by the Contracting Officer? 5. Is there obligated money for contract awards? 6. Have the risk limits of the Business Owner been defined and mitigation/contingency plans developed for the risks of highest impact? 7. Are the plans for the Requirements Analysis and subsequent phases realistic and achievable with the available resources? 8. Have all previously established approval conditions been satisfied?

Major Probing Questions for the Information Security Critical Partner	❖ Use the following questions to assist you with completing your responsibilities for this phase as appropriate to your subject matter expertise. Additional questions are located in the Additional Questions section of this manual. 1. What information security and privacy requirements have been identified, planned for and included in the Project Management Plan? 2. What issues and/or risks do you see that would affect the continuation of the project into the requirements phase and subsequent design, development, testing & implementation? 3. How completely have the Project Management Plan components been developed? 4. How well has compliance with Enterprise Architecture been maintained through the Planning Phase? 5. How well does the Requirements Traceability Matrix describe the way that the system design will satisfy the functional, business, information security, and technical specifications in the Requirements Document?

Role of an Information Security Critical Partner in Requirements Analysis Phase

Brief Description of Phase

The Requirements Analysis phase develops detailed functional and non-functional requirements and the Requirements Traceability Matrix (RTM) and award contracts if needed. The outcome of the Requirements Analysis Phase is award of required contracts and approval of the requirements.

Information Security Responsibilities

Deliverables (Project Planning & Execution) Lane 1	❖ Provide oversight, advice and counsel to the project manager to ensure that the Requirements Document addresses relevant information security and privacy standards. ❖ Ensure that an assessment of the required information security and privacy controls has been completed. ❖ Determine if requirements reflect alignment with established information security standards including the FIPS-199 Categorization and Accreditation Boundary. ❖ Ensure the assessment of required information security controls (per NIST guidelines) has been completed.

Project Reviews Lane 2	❖ Participate in the Requirements Review as appropriate to your subject matter expertise by providing information, judgment and recommendations to the Project Manager. ▪ Requirements Review purpose is to: 1. Ensure requirements are complete, accurate, consistent and problem-free 2. Evaluate responsiveness of the requirements to the business requirements 3. Ensure requirements are a suitable basis for subsequent design activities 4. Ensure traceability within the requirements and between the design documents 5. Affirm final agreement regarding the content of the Requirements Document

Stage Gate Reviews Lane 3	❖ Participate in the Requirements Stage Gate Review if requested by the National Center's IR Governance Plan and as appropriate to your subject matter expertise by providing a recommendation on the following Stage Gate Review questions: 1. Are the functional and non-functional requirements sufficiently detailed and grouped and so that the business need will be met and that the requirements can be tested once the product is developed? 2. Has the initial Test Plan been sufficiently defined? 3. Have process and data models been defined adequately for design? 4. Has the Project Management Plan along with its components been reviewed and appropriately updated based on the information

	acquired during the requirements analysis phase? 5. Are the highest impact risks being monitored and the mitigation/contingency plans updated as appropriate? 6. Have any variances from cost, schedule and performance baselines been identified and mitigated with plans for correction? 7. Are the plans for the Design and subsequent phases realistic and achievable with the available resources? 8. Have all previously established approval conditions been satisfied?

Major Probing Questions for the Information Security Critical Partner	❖ Use the following questions to assist you with completing your responsibilities for this phase as appropriate to your subject matter expertise. Additional questions are located in the Additional Questions section of this manual. 1. How thoroughly has the assessment of the required information security controls been completed, and how do they reflect alignment with established information security standards, including the FIPS-199 Categorization and Accreditation Boundary?? 2. Are plans complete to track technical changes? 3. What issues and/or risks do you see that would affect the continuation with the design phase and subsequent development, testing & implementation? 4. How well do the requirements provide a suitable basis for subsequent design activities? 5. Which, if any, of the technical and/or service standards that have been identified for this project will either facilitate or constrain solution design and development activities?

Role of an Information Security Critical Partner in Design Phase

Brief Description of Phase

The Design phase develops the Design Document. The outcome of the Design Phase is completion of Business Product design and successful completion of Preliminary and Detailed Design Reviews.

Information Security Responsibilities

Deliverables (Project Planning & Execution) Lane 1	❖ Participate in the making of tradeoff decisions if conflicting goals have arisen during the Design. ❖ Establish that information security documents (C&A, Privacy Impact Assessment, System of Record Notice, and Computer Match Agreement) are reviewed for completeness and accuracy and that Contingency/Disaster Recovery Plan includes complete procedures, arrangements and responsibilities. ❖ Verify that project information security risks are identified and mitigation plans are made and documented.

Project Reviews Lane 2	❖ Participate in the Detailed Design Review as appropriate to your subject matter expertise if requested by the National Center's IR Governance Plan or by the Project Manager. ▪ Detailed Design Review purpose is to: 1. Ensure individual design components (units/modules) of an automated system/application are completely defined and documented in sufficient detail 2. Verify how they interface with each other 3. Ensure design of the automated system/application is complete, fully integrated, and ready to move to the Development Phase 4. Ensure identified and open issues are resolved

Stage Gate Reviews Lane 3	❖ Participate in the Preliminary Design Stage Gate Review as appropriate to your subject matter expertise by providing a recommendation on the following Stage Gate Review questions: 1. Does the high-level architectural design satisfy the functional and non-functional requirements? 2. Is the high-level architectural design consistent with the CDC enterprise architecture? 3. Are there any technical or information security related issues or risks that would affect the continuation of a detailed design? 4. Has the Project Management Plan along with its components been reviewed and appropriately updated based on the information acquired during the Requirements Analysis Phase and preliminary design activities? 5. Are the highest impact risks being monitored and the mitigation/contingency plans updated as appropriate?

	6. Have any variances from cost, schedule and performance baselines been identified and mitigated with plans for correction? 7. Are the plans for the detailed design and subsequent phases realistic and achievable with the available resources? 8. Have all previously established approval conditions been satisfied?

Major Probing Questions for the Information Security Critical Partner	❖ Use the following questions to assist you with completing your responsibilities for this phase as appropriate to your subject matter expertise. Additional questions are located in the Additional Questions section of this manual. 1. How closely does the high-level architectural design conform to CDC information security requirements? 2. What issues and/or risks do you see that would affect the continuation with the detailed design and subsequent development, testing & implementation? 3. How completely does the Requirements Traceability Matrix describe how the system design will satisfy the functional, business, information security, and technical specifications in the Requirements Document?

Role of an Information Security Critical Partner in Development Phase

Brief Description of Phase

The Development phase develops code and other deliverables required to build the Business Product and conduct an Independent Verification & Validation Assessment. The outcome of the Development Phase is completion of all coding and associated documentation; user, operator and maintenance documentation, and test planning.

Information Security Responsibilities

Deliverables (Project Planning & Execution) Lane 1	❖ Provide oversight, advice and counsel to the project manager on the conduct and requirements of the Development phase. ❖ Ensure that all development plans address safety, information security, and privacy concerns. ❖ Validate that the test plan includes explicit testing of information security controls and functional capabilities. ❖ Confirm that the Systems Security Plan and the Security Risk Assessment address all required topics and that an IV&V assessment has been conducted.
Project Reviews Lane 2	❖ Participate in the Validation Readiness Review as appropriate to your subject matter expertise and if requested by the National Center's IR Governance Plan or by the Project Manager. ▪ Validation Readiness Review purpose is to: 1. Ensure that the software has completed thorough unit/module/software integration testing 2. Ensure that software is ready for turnover to the formal, controlled test environment where validation testing will be conducted ▪ The Independent Verification & Validation Assessment is conducted by an independent third party to: 1. Provide management with an independent perspective on the full scope of project activities, from planning through implementation 2. Identify potential improvements that may not be apparent to those working directly on the project 3. Identify problems before they occur and thus avoid loss and minimize the cost of any necessary corrective action
Stage Gate Reviews Lane 3	❖ Participate in the Development Stage Gate Review if requested by the National Center's IR Governance Plan and as appropriate to your subject matter expertise by providing a recommendation on the following Stage Gate Review questions: 1. Does the solution (Business Product) satisfy the requirements established and refined during the Requirements and Design Phases? 2. Does the Test Plan ensure that all test cases will be adequately

	evaluated and executed, and system tested to ensure requirements are met? 3. Are the information security plans and risk assessments complete and in compliance with regulatory requirements? 4. Has the Project Management Plan along with its components been reviewed and appropriately updated based on the information acquired during the development activities? 5. Are the highest impact risks being monitored and the mitigation/contingency plans updated as appropriate? 6. Have any variances from cost, schedule and performance baselines been identified and mitigated with plans for correction? 7. Are the plans for the Testing and subsequent phases realistic and achievable with the available resources? 8. Have all previously established approval conditions been satisfied?

Major Probing Questions for the Information Security Critical Partner	❖ Use the following questions to assist you with completing your responsibilities for this phase as appropriate to your subject matter expertise. Additional questions are located in the Additional Questions section of this manual. 1. Has the system been documented and modeled in the HHS EA Repository (HEAR), CDC's ProSight (PMT/OMB 300), SPORT (FISMA), Enterprise Systems Catalog (ESC) and HI.net? 2. How well do all development plans address safety, information security, and privacy concerns? 3. What explicit testing of information security controls and functional capabilities does the test plan include? 4. How complete are the Systems Security Plan and the Security Risk Assessment? 5. What issues and/or risks do you see that would affect the testing and subsequent implementation? 6. How complete are the Test Plans that address information security?

Role of an Information Security Critical Partner in Test Phase

Brief Description of Phase

The Test phase has thorough testing and auditing of the Business Product's design, coding and documentation. The outcome of the Test Phase is completed acceptance testing and readiness for training and implementation.

Information Security Responsibilities

Deliverables (Project Planning & Execution) Lane 1	❖ Review test procedures and outcome in the areas affecting information security. ❖ Validate penetration tests and vulnerability scans are executed, documented and any failed components are documented, and either mitigated and/or accepted as residual risk by the appropriate authority.

Project Reviews Lane 2	❖ Participate in the Implementation Readiness Review as appropriate to your subject matter expertise if requested by the National Center's IR Governance Plan or by the Project Manager. ▪ Implementation Readiness Review purpose is to: 1. Ensures that the IT solution or automated system/application is ready for implementation activities 2. 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)

Stage Gate Reviews Lane 3	❖ Participate in the Test Stage Gate Review if requested by the National Center's IR Governance Plan and as appropriate to your subject matter expertise by providing a recommendation on the following Stage Gate Review questions: 1. Does the solution (Business Product) satisfy the requirements established? 2. Has the test plan been executed as defined? 3. Do the testing results support the decision to move to the Implementation Phase? 4. Does the Implementation Plan provide sufficient detailed information on the move of the solution into production? 5. Is there an adequate "fall back" plan in place or other alternatives in the event of catastrophic failure? 6. Has the Project Management Plan along with its components been reviewed and appropriately updated based on the information acquired during the testing? 7. Are the highest impact risks being monitored and the mitigation/contingency plans updated as appropriate?

	8. Have any variances from cost, schedule and performance baselines been identified and mitigated with plans for correction? 9. Are the plans for the Implementation and subsequent phases realistic and achievable with the available resources? 10. Have all previously established approval conditions been satisfied?

Major Probing Questions for the Information Security Critical Partner	❖ Use the following questions to assist you with completing your responsibilities for this phase as appropriate to your subject matter expertise. Additional questions are located in the Additional Questions section of this manual. 1. Is this system being documented and modeled in the HHS EA Repository (HEAR), CDC's ProSight (PMT/OMB 300), SPORT (FISMA), Enterprise Systems Catalog (ESC) and HI.net? 2. How well do the validation tests confirm the information security of the Business Product? 3. What is the result of penetration tests and vulnerability scans, and what is the status any failed components that have been reworked? 4. What issues and/or risks do you see that would affect the continuation into the implementation phase and subsequent operations & maintenance? 5. How closely do approved change requests comply with the EA Technical Reference Model?

Role of an Information Security Critical Partner in Implementation Phase

Brief Description of Phase

The Implementation phase conducts user and operator training, determine readiness to implement, and execute the Implementation Plan, including any phased implementation. The outcome of the Implementation Phase is successful establishment of full production capability and completion of the Post-Implementation Review.

Information Security Responsibilities

Deliverables (Project Planning & Execution) Lane 1	❖ Provide oversight, advice and counsel to the project manager on the conduct and requirements of the implementation phase. ❖ Provide information, judgment, and recommendations to the Business Owner and IT governance organizations during project reviews and in support of Project Baselines. ❖ Determine if Plan of Objectives and Milestones, Authority to Operate, including the System Certification and Accreditation, is complete and System of Record Notice is published.

Project Reviews Lane 2	❖ Participate in the System Certification and Accreditation Reviews and Post Implementation Review as appropriate to your subject matter expertise if requested by the National Center's IR Governance Plan or by the Project Manager. ▪ System Certification purpose is to: 1. Conduct a comprehensive evaluation of the management, operational, and technical security controls 2. Ensure compliance with information security requirements 3. Review the Information Security Risk Assessment (IS 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 ▪ System Accreditation purpose is to: 1. Implement the most effective security controls, in consideration of technical, budgetary, time, and resource limitations, while continuing to support business mission requirements 2. Ensure 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 3. Ensure that the CIO/DAA explicitly accept or reject any identified residual risks to the organization's operations and assets remaining after the implementation of the prescribed set of security controls as documented in the SSP and/or IS RA 4. Ensure that the CIO/DAA 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 ▪ Post Implementation Review purpose is to: 1. Determine if the IT system is operating as expected 2. 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) 3. Examine the efficacy of all elements of the working business solution to see if further improvements can be made to optimize the benefit delivered 4. Learn lessons from the project that can be used to improve future project work and solutions

Stage Gate Reviews **Lane 3**	❖ Participate in the Operational Readiness Stage Gate Review as appropriate to your subject matter expertise by providing a recommendation on the following Stage Gate Review questions: 1. Is the solution ready for release into the production environment for sustained operations and maintenance support? 2. Has the Project Management Plan along with its components been reviewed and appropriately updated based on the information acquired during the testing and implementation phases? 3. Are the highest impact risks being monitored and the mitigation/contingency plans updated as appropriate? 4. Have any variances from cost, schedule and performance baselines been identified and mitigated with plans for correction? 5. Are the plans for the Implementation and Operations/Maintenance phase activities realistic and achievable with the available resources? 6. Have all previously established approval conditions been satisfied?

Major Probing Questions for the Information Security Critical Partner	❖ Use the following questions to assist you with completing your responsibilities for this phase as appropriate to your subject matter expertise. Additional questions are located in the Additional Questions section of this manual. 1. Has the system been documented and modeled in the HHS EA Repository (HEAR), CDC's ProSight (PMT/OMB 300), SPORT (FISMA), Enterprise Systems Catalog (ESC) and HI.net? 2. What is the status of the System Certification and the System Accreditation Project Reviews, and how have all issues been resolved? 3. What is the status of the Authority to Operate and the System of Record Notice? 4. What issues and/or risks do you see that would affect the production operation of the system?

	5. Has compliance with Enterprise Architecture been maintained throughout the approved change requests as a result of the Test and Implementation Phases? 6. What, if any, changes negatively impact dependencies with other systems? 7. Have the necessary infrastructure and associated products for the production environment been acquired, configured, and integrated?

Role of an Information Security Critical Partner in Operations & Maintenance Phase

Brief Description of Phase

The Operations & Maintenance phase operates and maintains the production system and conducts annual operational analyses. The outcome of the Operations and Maintenance Phase is successful operation of the asset against current cost, schedule and performance benchmarks.

Information Security Responsibilities

Deliverables (Project Planning & Execution) Lane 1	❖ Provide oversight, advice and counsel to the project manager on the conduct and requirements of the Operations and Maintenance phase. ❖ Determine if the Authority to Operate, System Certification and Accreditation and Privacy Impact Assessments are reviewed and updated at the appropriate times for continued operation. ❖ Ensure that Information Security documents are updated as necessary in response to continuous testing and monitoring. ❖ Confirm that system backups, physical security, contingency planning, and continuous information security monitoring and testing are operated in accord with established information security controls.

Project Reviews Lane 2	❖ Participate in the System Re-Certification and Re-Accreditation Reviews and Annual Operational Analysis as appropriate to your subject matter expertise and if requested by the National Center's IR Governance Plan or by the Project Manager. ▪ System Re-Certification purpose is to: 1. Ensure that the system is continuing to operate at an acceptable risk level ▪ System Re-Accreditation purpose is to: 1. Authorize continuation of the operation of an information system ▪ Annual Operational Analysis purpose is to: 1. Evaluate system performance 2. Determine user satisfaction with the system 3. Evaluate adaptability to changing business needs 4. Evaluate if new technologies might improve the system

Stage Gate Reviews Lane 3	❖ Participate in the Operations & Maintenance Stage Gate Review if requested by the National Center's IR Governance Plan and as appropriate to your subject matter expertise by providing a recommendation on the following Stage Gate Review questions: 1. Do the annual reviews provide sufficient data for a decision on whether enhancements or modifications are needed or whether the system (solution) should be replaced or disposed of? 2. Are the highest impact risks being monitored and the mitigation/contingency plans updated as appropriate?

	3. Have any variances from cost, schedule and performance baselines been identified and mitigated with plans for correction? 4. Are the plans for continued operations/maintenance activities realistic and achievable with the available resources? 5. Have all previously established approval conditions been satisfied?

Major Probing Questions for the Information Security Critical Partner	❖ Use the following questions to assist you with completing your responsibilities for this phase as appropriate to your subject matter expertise. Additional questions are located in the Additional Questions section of this manual. 1. Has the system been documented and modeled in the HHS EA Repository (HEAR), CDC's ProSight (PMT/OMB 300), SPORT (FISMA), Enterprise Systems Catalog (ESC) and HI.net? 2. How complete is the documented disposal/transition plan for closing or transitioning the system or its information? 3. What is the date of the Authority to Operate? 4. What issues and/or risks do you see that would affect the disposition of this project? 5. Which technologies used by this project are no longer needed within CDC?

Role of an Information Security Critical Partner in Disposition Phase

Brief Description of Phase

The Disposition phase retires the asset when operational analysis indicates that it is no longer cost-effective to operate the asset. The outcome of the Disposition Phase is the deliberate and systematic decommissioning of the Business Product with appropriate consideration of data archiving and security, migration of data or functionality to new assets, and incorporation of lessons learned over the project life cycle.

Information Security Responsibilities

Deliverables (Project Planning & Execution) Lane 1	❖ Handle transition reviews from the Information Security perspective. ❖ Guarantee that access authorities are removed, that data is properly migrated, and that all hardware and data storage devices have been sanitized to ensure no sensitive data is compromised.
Project Reviews Lane 2	❖ Note: There are no formal project reviews required during the Disposition Phase
Stage Gate Reviews Lane 3	❖ Participate in the Disposition Stage Gate Review if requested by the National Center's IR Governance Plan and as appropriate to your subject matter expertise by providing a recommendation on the following Stage Gate Review questions: 1. Are the data archiving, security, and data and systems migrations are complete? 2. Has the migration of data and the function to a new system been well-planned? 3. Has a final phase-end review has been conducted? 4. Have data ownership issues been addressed?
Major Probing Questions for the Information Security Critical Partner	❖ Use the following questions to assist you with completing your responsibilities for this phase as appropriate to your subject matter expertise. Additional questions are located in the Additional Questions section of this manual. 1. Where is the index of preserved information, including its location and retention attributes? 2. Was the Authority to Operate cancelled? 3. How complete are the media sanitization records? 4. What is the status of the disposition records for hardware and software (may include lists of hardware and software released – sold, discarded or donated – and lists of hardware and software redeployed to other projects or tasks within the organization)? 5. How has the project verified that all access authorities been removed? 6. Where has all the project data been migrated or archived? 7. How thoroughly have all hardware and data storage devices been

	sanitized to ensure no sensitive data is compromised? 8. Where is all the documentation archived, and is it complete?

Resources

The following list is a composite of resources to assist in conducting Stage Gate Reviews:

- CDC Enterprise Critical Partners as of 12/1/09. The names of these individuals may change over time; therefore, it is recommended that you visit the CPIC intranet site CDC http://intranet.cdc.gov/cpic/ for up-to-date individuals (coming soon)

Enterprise Architecture	Mike Perry & John Fitzpatrick
Security	Joseph Domingue & Kerey Carter
Acquisition Management	Terrance Perry & Gary Sentelle
Finance/Budget	Daniel J Hardee
Human Resources*	Angelia Jarrard & Debbie George
Section 508	Mark Urban
CPIC	Sandra McGill
Performance	Steve Racine

* the Atlanta Human Resources Center (AHRC) handles HR issues for Civil Service personnel; HR for Commissioned Corps personnel and Training for all personnel are handled by Office of Workforce and Career Development (OWCD) or its successor organizations

- CDC UP for definition and examples of documents and deliverables at all phases (http://www.cdc.gov/cdcup)
- CDC Information Technology Strategic Plan FY 2009 – 2013 for CDC IT goals; also includes appendices with
    - CDC Health Protection Goals
    - HHS Information Technology Strategic Plan Goals & Objectives 2006 -2010
- CDC Enterprise Architecture web site for CDC EA guiding principles (http://intranet.cdc.gov/ncphi/ea/ea_document_library.html)
- CDC Enterprise Systems Catalog for inventory of existing CDC systems (http://esc.cdc.gov/)
- CDC Financial Management Office (FMO) for budget formulation and appropriations guidance, budget execution, payments and executions, accounting, financial management systems, regulations/policies/procedures, and FMO Service Desk http://intra-apps.cdc.gov/fmo/)
- CDC HealthImpact.net for inventory of existing CDC projects (http://healthimpactnet.cdc.gov/)
- CDC policy and procedures related to Capital Planning and Investment Control (CPIC), including Earned Value Management (EVM) (http://intranet.cdc.gov/cpic/)
- CDC Office of Career Development (OWCD) for training considerations (http://intranet.cdc.gov/owcd/)

- CDC Office of Commissioned Corps Personnel for HR considerations for USPHS officers (http://www.cdc.gov/od/occp/)
- CDC Procurement and Grants (PGO) web site for contracts information and guidance (http://pgo.cdc.gov/pgo/ViewCategory.do?AudienceID=2) and IT Program Management Office (ITPMO) (http://pgo.cdc.gov/pgo/ViewCategory.do?AudienceID=4)
- CDC Section 508 guidance for web (http://intranet.cdc.gov/cdcweb/usability/508/)
- CDC Security information from OCISO (http://intranet.cdc.gov/ociso/)
- HHS Atlanta Human Resources Center (AHRC) for Civil Service HR considerations (http://intranet.cdc.gov/hr/index.html)
- HHS Enterprise Architecture Principles (http://www.hhs.gov/ocio/ea/architecture/index.html)
- HHS Portfolio Management Tool (PMT) – also known as ProSight – for descriptions of existing investments (https://pmt.hhs.gov/)
- HHS Enterprise Architecture Repository (HEAR) – also known as Troux Architect – for the architectural artifacts for existing Major and Tactical investments (see Enterprise EA Critical Partner for access information)
- Federal Acquisition Regulation (FAR) web site (http://www.arnet.gov/far/)
- Federal Enterprise Architecture web site for e-Government Initiatives and their architectures as described in the Federal Transition Framework (http://www.whitehouse.gov/omb/e-gov/fea/)
- Federal CIO Council: Architecture Principles for the U.S. Government (http://www.cio.gov/library/documents_details.cfm?id=Architecture%20Principles%20for%20The%20U.S.%20Government%20&structure=Enterprise%20Architecture&category=Enterprise%20Architecture)
- OMB Circular A-11 for description of the Exhibit 300 and Exhibit 53 (http://www.whitehouse.gov/omb/financial_offm_circulars/)

Stage Gate Assessment Tool

The Stage Gate Assessment Tool is currently being revised. Additional information will be available soon.

Bank of Additional Questions

The following are additional questions that might be raised to dig deeper into areas where less than satisfactory answers were provided to the major probing questions:

Initiation Phase	1. How does this project advance CDC or HHS goals? Is there an e-Government or HHS initiative with which this project would be redundant? Is this project consistent with the CDC IT Strategic Plan? 2. Is there a way to share, reuse, or modify an existing system without creating a new purpose-specific project? 3. What is the problem the project is trying to solve? What other organizations within CDC are facing the same problems and how have they addressed them? 4. Have the business requirements been reviewed with users and other stakeholders? 5. Who are the target users? What other CDC systems address the same users? 6. What are the top value-added features/services that this project will provide? Is this an innovative, more effective, or more efficient approach that could be leveraged by other CDC organizations? 7. In what environments will the IT solution operate? 8. What are the constraints on the IT solution?

Concept Phase / Project Selection Review	9. How does the project align with the CDC IT Strategic Plan and the HHS IT Strategic Plan? 10. Does the Project Charter give an adequate description of the product or IT solution to be developed by the project? 11. What are the high-level requirements for the project? Have the key functional requirements been summarized in a clear, concise priority order? 12. Is any aspect of this project/investment supporting an essential COOP business process?

Planning Phase / Project Baseline Review	13. Does it appear that an increase in information security funding is needed to remediate IT security weaknesses? 14. Has identifying and assessing information security and privacy risks been incorporated into the overall risk management planning? 15. Have the IT security cost for the investment/project been integrated in to the overall cost including (C&A/re-accreditation, system security plan, risk assessment, privacy impact assessment, configuration/patch management, security control testing and evaluation, and contingency planning/testing)? 16. Are the appropriate information security and privacy requirements included (or there is a plan to include the requirements) in all contracts. 17. Have contractor information security procedures been developed? 18. Have the applicable information security and privacy standards been identified and planned for?

Requirements Analysis Phase	19. Are the requirements detailed enough and with enough specificity enough to be measurable? 20. Has there been agreement by all stakeholders and the business owner on the requirements? 21. Have the major stakeholders provided the business requirements? 22. What has been done to determine the accuracy of the requirements? 23. What has been done to ensure that requirements are complete? 24. Are requirements suitable for subsequent design activities? 25. Has the assessment of required information security controls been completed? 26. Are meetings conducted with the End Users to elicit requirements? 27. Are the requirements testable? 28. Are there any requirements that appear contradictory, ambiguous or unclear? 29. Is there enough detail in the business requirements for an analyst to write a technical specification? 30. Can the business requirements be grouped into critical, major, minor, and nice-to-have categories? 31. What is the quality assurance process for the business requirements?

Design Phase / Preliminary Design Review	32. Do any of the approved change requests for the project require modification in cost, schedule, scope, or resources? 33. Have all stakeholders, including the end-user community, been kept informed and/or consulted as appropriate during the Design Phase? 34. Will the design facilitate the accomplishment of performance metrics? 35. Given the proposed design, will the budget be sufficient to meet the needs of the project completion? 36. Have the needs for user, system, maintenance, operations, and business training and/or documentation been considered in the design? 37. Does the design define the release strategy in sufficient detail? 38. Has the interface control been documented? 39. Does the Design Document provide an overview of the entire hardware and software architecture and data design, including specifications for external interfaces? 40. Has the Requirements Traceability Matrix been updated to describe how the system design will satisfy the functional, business, information security, and technical specifications in the Requirements Document? 41. Does the design include all lower-level detailed design specifications of the Business Product, such as general system characteristics, the logical and physical data model, user interfaces, and business rules? 42. Has the design addressed data conversion issues at the appropriate level? 43. Are information security control test completion dates for all systems associated with this project/ investment within the last 365 days? 44. Does the Contingency/Disaster Recovery Plan include complete descriptions of the strategy and courses of action if there is a loss of use of the established business product (e.g., system) due to factors such as

	natural disasters or system or information security failures? 45. If an existing Computer Match Agreement involves another Federal agency, has an Inter/Intra-agency Agreement (IA) been prepared? 46. If required, has a Computer Match Agreement been finalized to establish conditions, safeguards, and procedures for disclosing data?

Development Phase	47. Does the information security risk assessment include the identification of all threats to and vulnerabilities in the information system; the potential impact that a loss of confidentiality, integrity, or availability would have and the identification and analysis of information security controls? 48. Does the Security Risk Assessment provide a formal risk assessment including the analysis of the information security functional requirements and the identification of the protection requirements? 49. Does the Systems Security Plan describe the information security controls, as defined by the National Institute of Standards and Technology that are designed and implemented within the system? 50. Has static code analysis been performed to identify information security vulnerabilities?

Test Phase	51. As a result of the Test activities and the development of the Implementation Plan, do any of approved change requests for the project require modification in cost, schedule, scope, resources, or acquisition planning? 52. Were any applicable additional tests conducted to validate documentation, training, contingency plans, disaster recovery, and installation? 53. Has the final Implementation Plan been developed?

Implementation Phase / Operational Readiness Review	54. Has a Post-Implementation Review been conducted? 55. Are all required Service Level Agreement(s) (SLAs) and Memorandum(s) of Understanding (MOU) fully executed and in effect, specifying each party's requirements, responsibilities and period of performance including performance guarantees? 56. As a result of the Development activities, do any of approved change requests for the project require modification in cost, schedule, scope, resources, or acquisition planning? 57. Has an accurate Project Completion Report that describes any differences between proposed and actual accomplishments, documents lessons learned, provides a status of funds, and provides an explanation of any open-ended action items, along with a certification of conditional or final closeout of the development project, been developed and have the processes been implemented? 58. Has the Operations & Maintenance Manual been updated based on results from the Test Phase? 59. Are backup procedures and responsibilities well-designed and up-to-date? 60. Do all systems associated with this project/investment have a publicly posted privacy impact assessment (PIA)?

	61. Does the risk assessment include the identification of all threats to and vulnerabilities in the information system; the potential impact that a loss of confidentiality, integrity, or availability would have and the identification and analysis of information security controls? 62. Does the Security Risk Assessment provide a formal risk assessment including the analysis of the information security functional requirements and the identification of the protection requirements? 63. Has a System Certification, including both information security and technical certifications, that ensures compliance with information security requirements been successfully completed? 64. Has a System Certification, including management, operational, and technical information security certifications, ensures compliance with information security requirements been successfully completed? 65. Has the Contingency/Disaster Recovery Plan been updated based on results from the Development and Test Phases? 66. Has the System Accreditation decision resulted in an Authority to Operate (ATO) that has been formally executed by a formal declaration of the Designated Approving Authority (DAA)? 67. Has the Systems Security Plan been finalized to describe the information security controls, as defined by the National Institute of Standards and Technology that are designed and implemented within the system? 68. Have required corrective actions been initiated on any outstanding documents? 69. Is all publicly posted system of record notices (SORN) for all applicable systems associated with this project/investment up-to-date?

Operations & Maintenance Phase	70. Did the project meet its information security criteria? 71. Were there any information security breaches that serve as lessons learned from this project and that should be incorporated into guidance for future projects?

Disposition Phase	72. Have information security objectives, including secure data and system transfer, sanitization and disposal of media, been accomplished?