Department of Health and Human Services

Centers for Medicare & Medicaid Services
Office of Information Services

CMS Testing Framework Overview

Draft

Version 0.8

September 11, 2008

Table of Contents

List of Figures

List of Tables

1. Introduction

The Centers for Medicare & Medicaid Services (CMS) has identified the need for integrated, standardized testing life cycle processes and guidelines to be defined within the *CMS Integrated IT Investment and System Life Cycle Framework* (hereafter simply the "CMS IT Framework"). These testing guidelines will describe a framework of testing functions to be performed during the Development, Test, Implementation, and Operations and Maintenance (O&M) Phases of the Information Technology (IT) investment/system life cycle in the CMS development, test, implementation, and production environments to enable the consistent delivery of high quality, production-ready CMS business applications and infrastructure.

1.1 Purpose

The purpose of the *CMS Testing Framework Overview* (hereafter simply the "CMS Testing Framework") is to establish a consistent, repeatable CMS testing life cycle process and framework for business application and infrastructure testing functions, which will reduce business risk by promoting more predictable testing actions and results.

The CMS Testing Framework will help establish, define, and organize guidelines for testing new and existing CMS business applications and infrastructure prior to their deployment to a data center's production environment. The CMS Testing Framework establishes standard terminology, definitions, structure, deliverables, reviews, roles and responsibilities, and support tools for CMS business application and infrastructure testing functions to facilitate efficient, responsive, and secure use and operation of CMS business applications and infrastructure.

Utilizing the CMS Testing Framework will reduce CMS and Office of Information Services (OIS) organizational risk, facilitate better resource need forecasts, improve testing schedules, and lower the incidence of reactive break/fix episodes.

The CMS Testing Framework will guide the testing standards for all contractor task orders supporting CMS business applications and infrastructure. Through contractor compliance with these standards, CMS will ensure alignment by contractors with the CMS IT Framework.

1.2 Scope

This CMS Testing Framework identifies and describes the various testing functions that may be performed for a CMS business application or infrastructure project during the project's CMS IT Framework phases of Development, Test, Implementation, and O&M. This document also identifies the testing process deliverables and the readiness reviews that determine whether the project has successfully met the exit criteria for its current CMS IT Framework phase and is ready to enter the next phase.

This CMS Testing Framework clarifies organizational roles and responsibilities in support of business application and infrastructure testing, and briefly addresses testing tools and test data.

1.3 Audience

This document is intended for use by the executive leadership of CMS, CMS personnel, and CMS contractors/subcontractors responsible for the ownership, management, definition, implementation, and support of CMS business applications and infrastructure.

1.4 Document Organization

This document is organized as follows:

Table 1: Document Organization

Section	Purpose
Section 1: Introduction	Defines the purpose, scope, audience, and organization of this document.
Section 2: CMS Testing Framework Overview	Provides an overview of the business application and infrastructure testing functions, deliverables, reviews associated with the testing framework, as well as roles and responsibilities, testing tools, and test data.
Section 3: Development Testing	Defines the Development Testing functions for CMS business applications.
Section 4: Validation Testing	Defines the Validation Testing functions prescribed for CMS business applications and infrastructure.
Section 5: Implementation Testing	Defines the Implementation Testing functions prescribed for CMS business applications and infrastructure.
Section 6: Operational Testing	Defines the Operational Testing functions prescribed for CMS business applications and infrastructure.
Acronyms	Provides a list of acronyms used in this document.

2. CMS Testing Framework Overview

The CMS Testing Framework is comprised of numerous testing functions that may be conducted during the life cycle of a given business application or infrastructure project, based on the specific circumstances of the project.

During the Planning Phase of a business application or infrastructure project's life cycle, the project team shall determine for each of the testing functions prescribed in the CMS Testing Framework if the testing function is required or not required for the given project. Each of the prescribed testing functions should be documented in the project's Project Process Agreement (PPA), along with the following information:

- lifecycle phase during which the testing function will be performed;
- name of the organization that will lead the testing;
- name and role of the key organization(s) to participate in and/or support the testing;
- any caveats or expectations if the testing function is required for the project, or a justification for why the testing function is not required for the project.

Determination of the specific testing functions to be performed for a project will be dependent on, but not limited to, the following:

- type of project (i.e., business application or infrastructure);
- acquisition, development, and/or maintenance approach;
- whether or not the CMS business application or infrastructure is new, is experiencing a major change, is experiencing a maintenance change, or if the change is due to an emergency problem correction;
- intended use and audience for the business application or infrastructure; and/or
- project risk(s) and/or information security risk level.

Testing functions may be performed iteratively and repeatedly for a particular project based upon the project implementation process used and upon the quality of test results produced by the testing activities.

The project's overall testing approach/strategy shall be appropriately documented in a Test Plan(s), along with a detailed description of each of the planned tests. The Test Plan(s) should describe how the CMS Testing Framework will be applied to the project, and identify any deviations from the prescribed CMS Testing Framework. Key aspects of the testing approach should be documented, such as content, methodology, prioritization, and progression of testing activities.

For example, the project's testing methodology may identify the order by which the selected testing functions are to be performed during the life cycle, identify if some testing functions are to be combined for testing efficiencies, and/or identify how the selected testing functions will be

performed (i.e., the testing methods). The testing methods may include (but are not exclusive to) white box testing[1], black box testing[2], positive testing[3], and negative testing[4], influenced by factors such as project cost, schedule, risk, and architecture. From an architecture perspective, for example, an application implemented using a Service Oriented Architecture (SOA) would include a focus on testing the scenarios of how a service is used by the CMS business application. As much as possible, reuse of test plans, test cases, test scripts, and test data should be considered.

2.1 Categories of Testing

The CMS Testing Framework encompasses four main categories of testing during the integrated IT investment and system life cycle: Development Testing, Validation Testing, Implementation Testing, and Operational Testing.

- **Development Testing –** A set of testing functions performed within a development environment for a CMS business application. These testing functions will confirm:
    - The behavior of the smallest testable elements of the software, including both functionality and data; and
    - That the modules of the business application's implementation model operate properly when combined to execute a set of requirements.

  Development testing includes the business application testing functions of Unit Testing, Application Integration Testing, and Section 508 Testing.

- **Validation Testing –** A set of testing functions performed within a test environment to confirm that the CMS business application or infrastructure fulfills requirements, and ensures that all relevant systems and data can accomplish a business process correctly.

  For business applications, validation testing includes the business application testing functions of System Testing, Functional Testing, End-to-End Integration Testing, User Acceptance Testing (UAT), Regression Testing, and Section 508 Testing.

  For infrastructure, validation testing includes the infrastructure testing functions of Infrastructure Testing, Infrastructure Regression Testing, Application Regression Testing, and Section 508 Testing.

- **Implementation Testing –** A set of testing functions performed within an implementation environment to confirm that the CMS business application or

---

1 Testing a system's logical paths through the software by exercising specific sets of conditions and/or loops.

2 Testing a system's external behavior, without consideration of internal structure.

3 A test case that supports confirmation that a requirement is successfully met.

4 Also known as destructive testing. A test case that intentionally attempts to force the system to behave incorrectly, helping to uncover system risk.

infrastructure will operate in accordance with architectural and technical requirements of a production environment.

Implementation testing includes the business application and infrastructure testing functions of System Acceptance Testing, Performance & Stress Testing, Initial Security Test and Evaluation (ST&E), Final Integration Testing, and Initial Contingency Planning Testing.

- **Operational Testing –** A set of testing functions performed within a production environment to confirm that the CMS business application or infrastructure operates in accordance with architectural and technical requirements and guidelines in a production environment.

  Operational testing includes the business application and infrastructure testing functions of Production Ready Testing, Monitoring & Reliability Testing, Operational ST&E, Audits, and Operational Contingency Planning Testing.

2.2 Business Application Testing Overview

The CMS Testing Framework provides guidance about "what" testing is necessary for CMS business applications built on mainframe and mid-tier platforms, but not "how" that testing should be performed (i.e., a testing methodology). The CMS Testing Framework includes readiness reviews, which are control gates to exit one environment and to enter another environment.

Figure 1 depicts a conceptual view of the CMS Testing Framework for business application testing that identifies the following:

- the four CMS IT Framework lifecycle phases during which business application testing is a primary activity (i.e. Development Phase, Test Phase, Implementation Phase, and O&M Phase);
- the four categories of testing described previously in section 2.1 aligned with the corresponding lifecycle phases (i.e., Development Testing, Validation Testing, Implementation Testing, and Operational Testing);
- the respective business application testing functions aligned with the four main categories of testing:
  - Unit Testing, Application Integration Testing, and Section 508 Testing associated with Development Testing;
  - System Testing, End-to-End Integration Testing, Regression Testing, Functional Testing, UAT, and Section 508 Testing associated with Validation Testing;
  - System Acceptance Testing, Initial ST&E, Initial Contingency Planning Testing; Performance & Stress Testing, and Final Integration Testing associated with Implementation Testing; and

  - Production Ready Testing, Operational ST&E, Operational Contingency Planning Testing, Monitoring & Reliability Testing, and Audits associated with Operational Testing;
- the supporting testing environments (i.e., Development Environment, Test Environment, Implementation Environment, and Production Environment); and
- the three primary CMS IT Framework readiness reviews during which business application testing is a key contributing factor (i.e., Validation Readiness Review (VRR), Implementation Readiness Review (IRR), and Operational Readiness Review(ORR)).

As identified in Figure 1, the testing functions possibly performed for a new or modified CMS business application align with corresponding phases of the CMS IT Framework. This diagram, however, does not represent the specific sequence of testing activities, although one may infer a general flow by reading the diagram from left to right.

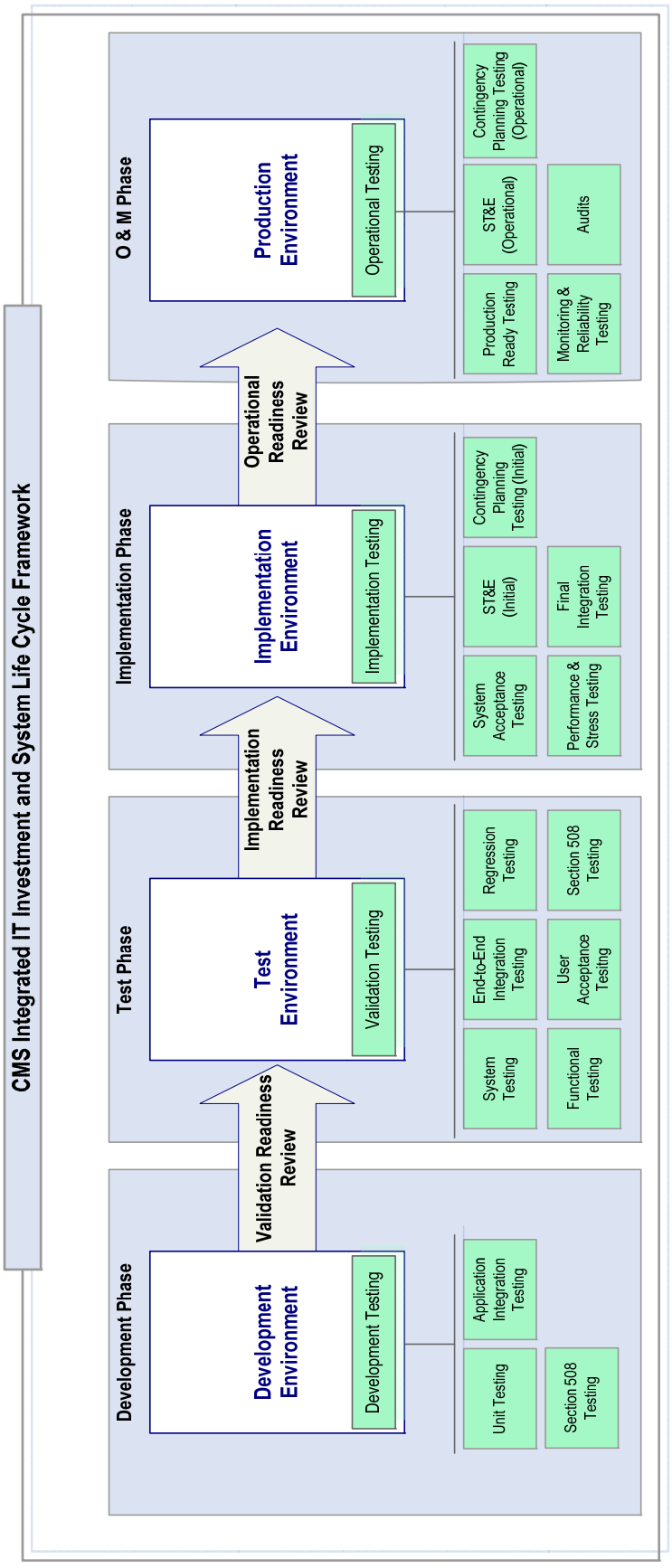

Figure 1: Business Application Testing Functions

2.3 Infrastructure Testing Overview

The CMS Testing Framework also provides guidance about "what" testing is necessary for new or modified infrastructure installed and configured on mainframe and mid-tier platforms, without prescribing the specific testing methodology to use. Within the CMS Testing Framework, *infrastructure* is deemed anything that is not a CMS business application. Therefore, infrastructure includes hardware, system software, data communications, and many other items that support CMS business applications running on the mainframe and mid-tier platforms.

Examples of infrastructure system software include an operating system such as Solaris, a database management system such as DB2, or Web server software used to host CMS Intranet Web applications. A change to infrastructure may include, for example, an upgrade of an operating system to a more current version; installation of a patch to Commercial Off-the-Shelf (COTS) software or utility; a change to a driver, utility, or firmware; or an upgrade to a board or Central Processing Unit (CPU).

The CMS Testing Framework includes readiness reviews, which are control gates to exit one environment and to enter another environment. Figure 2 depicts a conceptual view of the CMS Testing Framework for infrastructure testing that identifies the following:

- the three CMS IT Framework lifecycle phases during which infrastructure testing is a primary activity (i.e. Test Phase, Implementation Phase, and O&M Phase);
- the three categories of testing described previously in section 2.1 aligned with the corresponding lifecycle phases (i.e., Validation Testing, Implementation Testing, and Operational Testing);
- the respective infrastructure testing functions aligned with the three categories of testing:
    - Infrastructure Testing, Infrastructure Regression Testing, Application Regression Testing, and Section 508 Testing associated with Validation Testing;
    - System Acceptance Testing, Initial ST&E, Initial Contingency Planning Testing; Performance & Stress Testing, and Final Integration Testing associated with Implementation Testing; and
    - Production Ready Testing, Operational ST&E, Operational Contingency Planning Testing, Monitoring & Reliability Testing, and Audits associated with Operational Testing;
- the supporting testing environments (i.e., Test Environment, Implementation Environment, and Production Environment); and
- the two primary CMS IT Framework readiness reviews during which infrastructure testing is a key contributing factor (i.e., IRR and ORR).

As identified in Figure 2, the testing functions possibly performed for new or modified infrastructure align with corresponding phases of the CMS IT Framework. This diagram does not represent the specific sequence of testing activities, although one may infer a general flow by reading the diagram's testing function boxes from left to right.

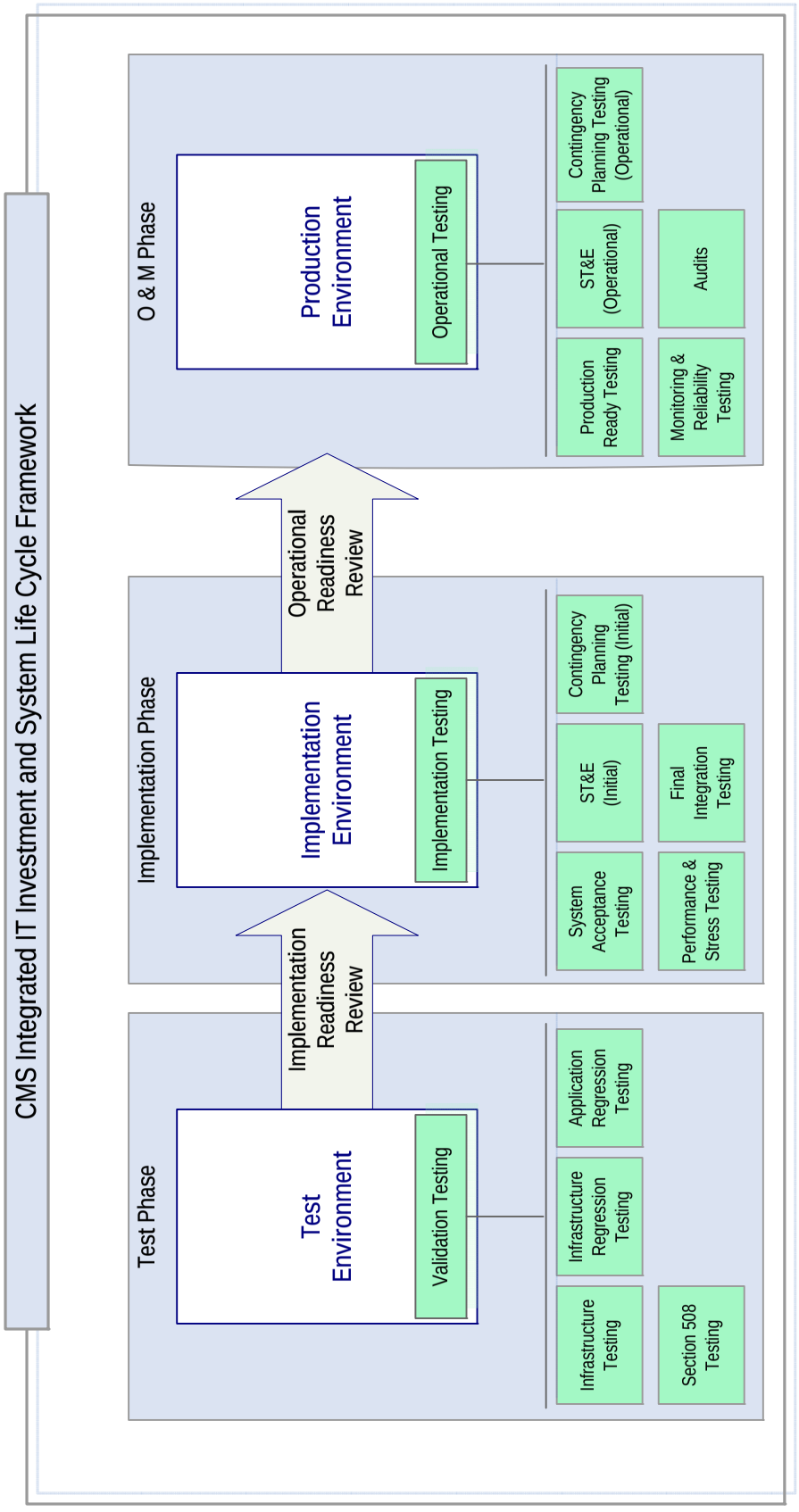

Figure 2: Infrastructure Testing Functions

2.4 Deliverables

Table 2 identifies the various deliverables prescribed by the CMS IT Framework and their specific role in the CMS Testing Framework.

Table 2: Role of CMS IT Framework Deliverables in the CMS Testing Framework

Deliverable	Role in CMS Testing Framework
Business Product/Code	The primary result from the development effort that satisfies the established requirements. In software development efforts, it includes the original source code and machine-compiled, executable computer instructions, and data repository(ies), that are the primary object of the testing.
Change Request (CR)	A formal document used to request a modification to specified software components, hardware, or documents that is managed through an established change control process. Each CR should be properly tested throughout the various phases of its life cycle.
Contingency Plan (CP)	Describes the strategy for ensuring system recovery in accordance with stated recovery time and recovery point objectives. CMS CP tabletop testing is required to be done annually for CMS business applications and infrastructure. The primary objective of the tabletop test is to ensure that designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner.
Corrective Action Plan (CAP)	Used to track the status of a finding from the execution of the Initial or Operational ST&E testing functions. A CAP provides a brief description of a finding, including the risk level (high, medium, or low) and the scheduled closing date, as well as other information pertaining to the finding.
Database Design Document	Describes the design of a database and the software units used to access or manipulate the data. Used in test planning and in the generation of test data and test cases.
Data Conversion Plan	Describes the strategies involved in converting data from an existing system/application to another hardware and/or software environment. It includes an inventory and cross reference of source and target data elements, schema, metadata and all self-describing files; process for data extraction, transformation and loading for each data source; tools needed to execute the conversion; and strategy for data quality assurance and control. Used in test planning and the generation of test data and test cases.

Deliverable	Role in CMS Testing Framework
Implementation Plan	Describes how the automated system/application or IT situation will be installed, deployed and transitioned into an operational system or situation. Used as a reference in conducting Implementation Testing and Operational Testing.
Information Security Risk Assessment (IS RA)	Contains a list of system threats and vulnerabilities, an evaluation of current system security controls, their resulting risk levels, and any recommended safeguards to reduce the system's risk exposure. Required for an ST&E.
Interface Control Document (ICD)	Describes the relationship between a source system and a target system. The ICD governs the data exchanged between the two systems and provides information describing the data exchange syntax and semantics that have been agreed upon for use. Used in test planning and in the generation of test data and test cases.
Operations and Maintenance (O&M) Manual	Clearly describes the automated system or application that will be operating in the production environment and provides the operations and support staff with the information necessary to effectively handle routine production processing, ongoing maintenance, and identified problems/issues. Used as a reference in conducting Implementation Testing and Operational Testing.
Problem Report (PR)	A formal document used to record an unexpected result that occurs during formal testing, implementation, or operation of the specified software or hardware. A PR is managed through an established process that includes investigation, resolution, and verification.

Deliverable	Role in CMS Testing Framework
Project Process Agreement (PPA)	Documents the process details for the project. Used to authorize and document the justifications for using, not using, or combining specific stage gate reviews and the selection of specific deliverables applicable to the investment/project, including the expected detail to be provided. Serves as a scope management tool for establishing the "Rules of Engagement" for the project, and assists in clarifying the requirements of the associated Statement of Work and resolving any potential ambiguities. Once approved by CMS, this document establishes the expectations and/or exceptions for the remainder of the project. It documents the deliverables and reviews required and not required by the project; the organization responsible for preparing the deliverable or participating in the review, frequency of delivery or occurrence, and other associated expectations, caveats, or justifications. It also documents the testing functions expected and not expected to be performed, the organization that will lead the testing, and the key organization(s) to participate in and/or support the testing along with their identified role, and other associated expectations/justifications.
Project Schedule	Documents the planned dates for performing the tasks and for meeting the milestones that comprise a project, including all test-related tasks and milestones. The Project Schedule includes identification of anticipated task durations, resources assigned to the tasks, and relationships to predecessor and successor tasks.
Release Plan/Release Management Plan	Describes what portions of the system functionality will be implemented in which releases and the rationale for each release.
Requirements Document	Defines the requirements that are to be tested. Used in test planning and the generation of test cases, test data, and a requirements-to-test case traceability matrix.
Section 508 Product Assessment	The mechanism for providing information regarding an electronic and information technology (EIT) product's compliance with the accessibility standards set forth by the Federal Access Board, which are the technical and functional provisions and performance criteria by which compliance with Section 508 of the Rehabilitation Act of 1973, as amended, are determined. Used in test planning and the generation of test cases and test data.

Deliverable	Role in CMS Testing Framework
System Design Document (SDD) w/ Requirements Traceability Matrix and CMS Section 508 Product Assessment	Describes how the system requirements recorded in the Requirements Document, preliminary functional and technical design recorded in the Business Process Models and High-Level Technical Design Concept/Alternatives, and the preliminary data design documented in the Logical Data Model are transformed into more technical system design specifications from which the system will be built. The SDD is used to document both high-level system design and low-level detailed design specifications, and is typically created in two increments. Used in test planning and in the creation of test data and test cases.
System Security Plan (SSP)	As required by the Federal Information Security Management Act (FISMA) of 2002, all information systems that store or process sensitive information must be covered by a SSP. The SSP contains descriptions of the actual managerial, technical and operational controls, documenting the current level of security implemented within the system. Used in test planning and in the creation of test data and test cases.
Test Plan	Describes the overall scope, technical and management approach, resources, and schedule for all intended test activities associated with testing a CMS business application or infrastructure. The Test Plan describes the items to be tested, the testing tasks to be performed, the personnel responsible for each task, the schedule and required resources for the testing activities, and the risks associated with the test plan that require contingency planning. More than one Test Plan may be prepared to address a specific testing function (e.g., a separate detailed ST&E Test Plan may be prepared and referenced in the main Test Plan).
Test Case Specification	Describes the purpose of a specific test, identifies the required inputs and expected results, provides step-by-step procedures for executing the test, and outlines the pass/fail criteria for determining acceptance. Individual tests are performed in accordance with the prescribed Test Case Specifications.
Test Incident Report (TIR)	Describes in detail the unexpected results, problems, or defects reported during testing, along with their documented resolutions. Generally included in an appendix to the Test Summary Report.

Deliverable	Role in CMS Testing Framework
Test Summary Report(s)	Documents the results from the various tests performed. Multiple reports may be generated during a project's life cycle (e.g., a Test Summary Report may be generated at the end of Development Testing, at the end of Validation Testing, and at the end of Implementation Testing). Separate Test Summary Reports may also be prepared for individual test functions (e.g., ST&E, UAT, and Section 508).
Training Artifacts	Include instructor and student guides, audio-visual aids, and computer-based or web-based software used to disseminate information about an automated system/application or other Information Technology (IT) solution to the target audience that is in need of the instruction. Usability and accessibility tested during Validation Testing.
User Manual	Clearly explains how a novice business user is to use the automated system or application from a business function perspective. Usability and accessibility tested during Validation Testing.
Version Description Document (VDD)	The primary configuration control document used to track and control versions of software being released to testing, to implementation, or to the final operational environment. The VDD provides a summary of the features and contents for a specific software build or release, and facilitates product implementation, testing, operations and maintenance. May reference Test Summary Report(s) as appropriate, or include a description of previous testing activities that were performed during the development of the system build and the corresponding test results (especially tests that cannot be performed in subsequent environments). If testing was limited for certain conditions, the VDD may identify those limitations for consideration during subsequent testing activities.

Detailed descriptions that further describe the purpose, document lifecycle, audience, roles and responsibilities, related deliverables, relationship to CMS IT Framework reviews, and other available guidance, as well as templates for these various deliverables are available from within the CMS IT Framework website located at: http://www.cms.hhs.gov/SystemLifecycleFramework/.

2.5 Reviews

Reviews are the CMS IT governance mechanism for management control and direction, decision making, coordination, confirmation of successful performance of activities, and determination of a CMS business application's or infrastructure's readiness to proceed to subsequent testing functions. Decisions made at each review will dictate the next step(s) for the business

application or infrastructure project and may include allowing the project to proceed to subsequent testing functions, directing rework before proceeding to the next environment and its associated testing functions, or terminating the project. Depending upon the systems development methodology employed (e.g., waterfall, spiral, iterative) and/or issues encountered during the lifecycle, projects may be scheduled to pass through a review more than once.

Table 3 identifies various reviews prescribed by the CMS IT Framework and their specific role in the CMS Testing Framework.

Table 3: Role of CMS IT Framework Reviews in the CMS Testing Framework

Review	Role in CMS Testing Framework
Project Baseline Review (PBR)	A formal inspection of the entire project and performance measurement baseline initially developed for the IT investment/project. The PBR is conducted to obtain management approval that the scope, cost, and schedule that have been established for the project are adequately documented and that the project management strategy is appropriate for moving the project forward in the life cycle. Upon successful completion of this review, the Project Schedule, Project Management Plan, and Project Process Agreement are baselined, which include the initial high-level plans for testing (i.e., identification of applicable testing functions, scheduling of testing activities, etc.).
Requirements Review	Establishes the baseline set of requirements that serve as the basis for test planning, the generation of test data and test cases, and subsequent testing activities.

Review	Role in CMS Testing Framework
Preliminary Design Review (PDR)	A formal inspection of the high-level architectural design of an automated system, its software and external interfaces, which is conducted to achieve agreement and confidence that the design satisfies the functional and nonfunctional requirements and is in conformance with the enterprise architecture. Overall project status, proposed technical solutions, evolving software products, associated documentation, and capacity estimates are reviewed to determine completeness and consistency with design standards, to raise and resolve any technical and/or project-related issues, and to identify and mitigate project, technical, security, and/or business risks affecting continued detailed design and subsequent development, testing, implementation, and operations & maintenance activities.
Validation Readiness Review (VRR)	Conducted to provide assurance that the software that is about to enter validation testing has completed development testing and is ready for turnover to the formal, controlled test environment where validation testing will be conducted. The scope of the VRR is to inspect the test products and test results obtained during development testing for completeness and accuracy, and to verify that test planning, test cases, scenarios, and scripts provide adequate coverage of documented system requirements. In addition, a review of the test environment, test setup, and test data is performed to ensure they are adequately prepared for validation testing.
Implementation Readiness Review (IRR)	Conducted to ensure that the IT solution or automated system/application that has been developed is ready for implementation activities, such that the required system hardware, networking and telecommunications equipment; COTS, GOTS, and/or custom-developed software; and database(s) can be installed and configured in the production environment(s). The results from validation testing serve as input to the IRR and the decision to proceed with implementation testing.

Review	Role in CMS Testing Framework
System Certification	The comprehensive evaluation of the management, operational, and technical security controls implemented for an information system to ensure compliance with information security requirements. The certification evaluation includes review of the IS RA, SSP, other system life cycle documentation, and any findings from past assessments, reviews and/or audits, as well as technical testing and analysis. The results of the initial technical certification assessment (ST&E), together with a review of any other independent audits, reviews or assessments are documented and appropriate corrective action is taken to strengthen internal controls. The SSP and/or IS RA are then updated based upon improvements and changes made to the system, and then the system is certified (approved) prior to subsequent System Accreditation.
System Accreditation	The official management decision by the CMS Chief Information Officer (CIO) / Designated Approval Authority (DAA) to authorize operation of an information system based on 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.
Operational Readiness Review (ORR)	A formal inspection conducted to determine if the final IT solution or automated system/application that has been developed or acquired, tested, and implemented is ready for release into the production environment for operational testing and sustained operations and maintenance support.

Review	Role in CMS Testing Framework
System Re-Certification	The comprehensive re-evaluation of the management, operational, and technical security controls implemented for an information system that is performed during the Operations & Maintenance Phase to ensure that the system is continuing to operate at an acceptable risk level. The results of an operational technical certification assessment (ST&E), together with a review of any other independent audits, reviews or assessments are documented and appropriate corrective action is taken to strengthen internal controls. The SSP and/or IS RA are then updated based upon improvements and changes made to the system, and then the system is certified (approved) prior to subsequent System Re-Accreditation.
System Re-Accreditation	The official management decision to authorize continued operation of an information system after acceptable System Re-Certification and any necessary adjustments have been completed.
IV&V Assessment	An assessment of a project's or a contractor's progress, products, and/or processes for a CMS business application or infrastructure conducted by an independent third party. IV&V may be performed for a business application or infrastructure at any time during the life of an investment/project by an organization that is technically, managerially, and financially independent of the CMS business owner, the system developer/maintainer, or other identified entity directly involved in supplying the product or performing the process. IV&V may be performed for any of the test-related activities, deliverables and/or processes.

Detailed descriptions for these various reviews are available from within the CMS IT Framework Website located at: http://www.cms.hhs.gov/SystemLifecycleFramework/.

2.6 Roles and Responsibilities

Multiple individuals and components from within CMS and other contractor organizations may have defined roles and responsibilities associated with business application and infrastructure testing activities, deliverables, and reviews. Specific roles and responsibilities will be

determined based on the circumstances of a given project and should be documented in the project's PPA.

Table 4 identifies various roles prescribed by the CMS IT Framework and their general role in the CMS Testing Framework.

Table 4: CMS Testing Framework Roles & Responsibilities

Role	Responsibilities in CMS Testing Framework
Business Owner	Conducts business application UAT to validate system requirements are met, which may be facilitated by a Testing Contractor. Certifies that the information system fully complies with FISMA security requirements and ensures appropriate security measures and supporting documentation are maintained. Ensures Contingency Planning Testing is conducted, which may be facilitated by a Testing Contractor.
Project Manager	Ensures that project deliverables are appropriately developed, if designated as being required per the PPA. Monitors the testing activities in accordance with test plans and the project schedule, and provides appropriate status reporting as needed. Ensures that the testing schedule is integrated into the master project schedule. Ensures that all appropriate business stakeholders and technical experts are involved throughout the life cycle of the IT investment/project.
Project Officer / Government Task Leader (GTL)	Ensures that the contractor satisfies the requirements of the Statement of Work (SOW) or Task Order (TO).
System Developer or System Maintainer	CMS organization or contractor developing a new or maintaining an existing CMS business application. Generally responsible for test planning and generation of test data and test case specifications for business application testing. At a minimum, responsible for performing Development Testing functions and also generally responsible for Validation Testing functions.
CMS IT Governance Organization	Conducts formal reviews as part of the CMS IT governance process (e.g., the Technical Review Board (TRB) conducts the PDR).

Role	Responsibilities in CMS Testing Framework
ESD Engineering Review Panel (ERP) [for ESD IDIQ Contract Task Orders only]	Reviews project deliverables and provide input to CMS regarding identified issues, risks, or actions requiring further consideration or modification. Also provides input to the TRB regarding any IT engineering and technology issues and challenges that may affect the transition of the Business Product/Code release into the target test, implementation, or production environment.
OIS Stakeholders (e.g., ISDDG, BAMG, EDCG, EDG, EASG, etc.)	Participates in test planning and test activities as necessary. ISDDG and BAMG conduct the VRR for business applications they manage. EDCG conducts the IRR and ORR, with input from other OIS stakeholders and subject matter experts as needed.
Testing Contractor	May perform one or more specific testing functions that include the definition (as needed), setup, and execution of test plans and test case specifications, and documenting and tracking test results. Generally not responsible for any Development Testing functions.
IT Infrastructure Implementation Agent or Contractor	Supports CMS development, testing, and production environment infrastructure. Generally performs a CMS business application's Implementation Testing and Operational Testing functions, with the exception of ST&E and Contingency Planning Testing. For infrastructure testing, generally performs Validation Testing, Implementation Testing, and Operational Testing functions, with the exception of Application Regression Testing, Section 508 Testing, ST&E, and Contingency Planning Testing.
IV&V Contractor	Conducts IV&V Assessments. Technically, managerially, and financially independent of any party affiliated with the business application or infrastructure being tested. Identifies potential improvements or identifies problems before they occur. At a minimum, generally performs initial and operational ST&E testing functions.

Role	Responsibilities in CMS Testing Framework
Configuration (or Change) Control Board (CCB)	Approves changes for release into production for a maintenance release delivered during the O&M Phase (e.g., validates the CRs incorporated in the release). May assist in test planning and review of test results for the CRs.

2.7 Testing Tools

CMS advocates the use of specific tools for the testing process. The list of prescribed tools is identified in the *CMS Technical Reference Architecture, Appendix A. CMS Products/Standards Selection List*.

2.8 Test Data

As prescribed by the *Federal Information Security Management Act* (FISMA) and the *CMS Policy for the Information Security Program* (PISP), if a testing environment contains data that includes real Personally Identifiable Information (PII) or Personal Health Information (PHI) then the testing environment must be secured with similar rigor as provided to a production environment. An alternate approach is to mask out PII/PHI data that is stored in the testing environment (i.e., redact the test data).

3. Development Testing

The business application Development Testing functions (Unit Testing, Application Integration Testing, and Section 508 Testing) will be performed to verify that an individual module and integrated sets of modules in a business application, and system components such as databases, hardware, software, or communication devices, behave as prescribed in the application solution's functional, data, technical, and architectural requirements.

The results of the Development Testing will be included in the VDD (either directly or by reference to a separate Test Summary Report) for the specific system build or release that is being transitioned into subsequent Validation Testing.

3.1 Unit Testing

Unit Testing is performed by the system developer/maintainer subsequent to or in parallel with application development to assess and correct the functionality and data of a business application's individual code modules.

3.2 Application Integration Testing

Application Integration Testing is preliminary testing performed by the system developer/ maintainer to assess the interfaces, data, and interoperability of modules and systems within a single business application. This testing function is sometimes also referred to as String Testing or Integration Testing.

If the business application requires data conversion, this testing function will include data conversion testing, as prescribed by the Data Conversion Plan.

3.3 Section 508 Testing

Section 508 Testing is performed by the system developer/maintainer to ensure that the EIT product is compliant with applicable Section 508 Accessibility Standards identified in the completed Section 508 Product Assessment. Software products (whether COTS, Government Off-the-Shelf (GOTS), or custom-developed software applications) must adhere to Section 508 accessibility and other regulatory requirements governing the use of EIT in accordance with the *CMS Policy for Section 508 Compliance*. Section 508 Testing is required if the business application has a user interface or produces electronic output for direct access or use by federal employees or the public.

4. Validation Testing

Validation Testing functions are performed for both business application testing and infrastructure testing, but differ in the testing functions that are conducted.

4.1 Business Application Validation Testing Functions

The system developer/maintainer or a testing contractor will perform the business application Validation Testing functions to validate that a business application and integrated system components (e.g., databases, hardware, software, or communication devices) behave as prescribed in the application's functional, data, technical, and architectural requirements.

4.1.1 System Testing

The system developer/maintainer or a testing contractor will perform System Testing to assess the functionality and interoperability of a business application and multiple systems, such as databases, hardware, software, or communication devices, and their integration with infrastructure into an overall integrated system. System Testing, which could be considered as "bottom-up" testing, includes a test installation and configuration of the business application, with a subsequent functional regression test to confirm the installation's success.

If the business application requires data conversion, this testing function will include data conversion testing, as prescribed by the Data Conversion Plan.

4.1.2 Functional Testing

A testing contractor will perform Functional Testing to assess the input/output functions of a business application against pre-defined functional and data requirements.

4.1.3 End-to-End Integration Testing

End-to-End Integration Testing will be a collaborative testing effort by a testing contractor, CMS IT Infrastructure Implementation Agent or Contractor, the business application's project manager (e.g., GTL), and affected business owners to confirm that the solution works correctly from end to end. End-to-End Integration Testing tests all of the business application's access or touch points, and data, across multiple business applications and systems, front to back (horizontal) and top to bottom (vertical), to ensure business processes are successfully completed. Testing will be conducted on a complete, integrated set of business applications and systems to evaluate their compliance with specified requirements, and to evaluate whether the business applications and systems interoperate correctly, pass data and control correctly to one another, and store data correctly. This testing function is sometimes referred to as Interface Testing.

4.1.4 User Acceptance Testing

The business owner will perform User Acceptance Testing (UAT) with support from a testing contractor to assess and accept the overall functionality and interoperability of a business application's solution in an operational mode. UAT allows end users to use the solution in a manner that most resembles actual production use. This testing will be performed against the Business Product/Code based on the user's requirements, and may include Training Artifacts and User Manual, if applicable to the project. If the business application has a user interface, UAT may also assess the user's experience with the application to determine if users are able to accomplish their tasks and goals satisfactorily and efficiently to help identify potential problems and possible improvements (i.e., usability testing). Success in UAT will result in a sign-off by the business owner, validating that the business application meets requirements.

4.1.5 Regression Testing

A testing contractor will perform Regression Testing, which will be selective re-testing of a business application to validate that modifications have not caused unintended functional or data results and that the application still complies with its specific requirements. This testing function is sometimes referred to as System Regression Testing.

4.1.6 Section 508 Testing

A testing contractor will perform Section 508 Testing to ensure that the EIT product is compliant with applicable Section 508 Accessibility Standards identified in the completed Section 508 Product Assessment. Software products (whether COTS, GOTS, or custom-developed software applications) must adhere to Section 508 accessibility and other regulatory requirements governing the use of EIT in accordance with the *CMS Policy for Section 508 Compliance*. Section 508 Testing is required if the business application has a user interface or produces electronic output for direct access or use by federal employees or the public.

4.2 Infrastructure Validation Testing Functions

The CMS IT Infrastructure Implementation Agent or Contractor, and possibly the testing contractor, will perform the infrastructure Validation Testing functions. The infrastructure Validation Testing will ensure that new or modified infrastructure (and business applications potentially affected), and such integrated system components as databases, hardware, software, or communication devices, behave as prescribed by the infrastructure's technical and architectural requirements.

4.2.1 Infrastructure Testing

The CMS IT Infrastructure Implementation Agent or Contractor will perform Infrastructure Testing to assess the interfaces and interoperability of new or modified infrastructure with other infrastructure and system components, such as databases, hardware, software, or communication devices.

4.2.2 Infrastructure Regression Testing

The CMS IT Infrastructure Implementation Agent or Contractor will perform Infrastructure Regression Testing to assess whether or not new or modified infrastructure causes unintended effects on other infrastructure that depend upon the new or modified infrastructure.

4.2.3 Application Regression Testing

Testing contractors will perform Application Regression Testing to assess whether or not new or modified infrastructure has negatively affected business applications that depend upon the infrastructure.

4.2.4 Section 508 Testing

A testing contractor will perform Section 508 Testing to ensure that the EIT product is compliant with applicable Section 508 Accessibility Standards identified in the completed Section 508 Product Assessment. Software products (whether COTS, GOTS, or custom-developed software applications) must adhere to Section 508 accessibility and other regulatory requirements governing the use of EIT in accordance with the *CMS Policy for Section 508 Compliance*. Section 508 Testing is required if the infrastructure has a user interface or produces electronic output for direct access or use by federal employees or the public.

5. Implementation Testing

Business application and infrastructure Implementation Testing functions will be performed to ensure that a business application or infrastructure solution behaves as required in a production-like environment, that it is configured with the same infrastructure as found in the target production environment, that it has the same security settings, and that it complies with the *CMS Technical Reference Architecture* (TRA). A business application or infrastructure solution that does not conform to production standards in design, architecture, configuration, and performance will be returned to the development test environment for correction.

5.1 System Acceptance Testing

The CMS IT Infrastructure Implementation Agent or Contractor will perform System Acceptance Testing on a business application or infrastructure to assess the solution's functionality, architecture, and configuration in a production-like environment. This testing will include a test of the installation procedures and configuration of the solution in the implementation test environment, with subsequent Application Regression Testing performed to confirm the installation's success.

System Acceptance Testing may include testing of startup and shutdown procedures and scripts, and backup and restore procedures and scripts, as described in the O&M Manual. The scope of System Acceptance Testing will include testing of the application or infrastructure solution against storage and processing requirements, communications, security, database, and other dimensions of systems operations necessary to perform effectively in a production environment. This testing function is sometimes referred to as Operational Validation Activities.

If the business application requires data conversion, this testing function will include data conversion testing, as prescribed by the Data Conversion Plan.

5.2 Performance & Stress Testing

The CMS IT Infrastructure Implementation Agent or Contractor will perform Performance and Stress Testing on a business application or infrastructure, supported by a testing contractor and the system developer/maintainer for a business application. Performance testing assesses the capacity and throughput of a business application or infrastructure in processing time, CPU utilization, network utilization, and memory and storage capacities relative to expected normal (average and peak) user and processing load. Stress testing exercises the business application or infrastructure with a large volume of input data and/or a large number of simulated users (i.e., "load") to determine maximum resource utilization at point of failure, in terms of processing time, CPU utilization, network utilization, and memory and storage capacities.

The same performance and stress testing tools on the respective mid-tier and mainframe platforms should be used for all business applications and infrastructure to ensure consistent test results relative to expected application behavior in a production environment.

Performance testing may include "Compatibility Testing," which tests the integration of the business application or infrastructure with other business applications, infrastructure, and systems already running in the environment in order to identify any resource contention, such as conflicts in ports or database record-locking contention.

5.3 Initial ST&E

An Initial ST&E will be performed by an IV&V or independent testing contractor for a business application or infrastructure. Initial ST&E determines the extent to which the security controls in the business application or infrastructure are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the application or infrastructure. Initial ST&E may include vulnerability scanning, penetration testing, and/or testing security standards and policy.

For new business applications or infrastructure, business applications or infrastructure with a major change, or security incidents, an Initial ST&E must be done in accordance with the *CMS Policy for the Information Security Program* in the implementation environment before the business application or infrastructure moves into a production environment.

For more detailed guidance, reference CMS' Information Security testing procedures available at: http://www.cms.hhs.gov/InformationSecurity/15_Procedures.asp#TopOfPage.

5.4 Final Integration Testing

Final Integration Testing will be a collaborative testing effort by the CMS IT Infrastructure Implementation Agent or Contractor, testing contractor, and by the application's project manager (e.g., GTL), and affected business owners for a business application or the Enterprise Data Center Group (EDCG) for infrastructure, to confirm that a business application or infrastructure solution works correctly from end to end in an environment configured the same as a production environment and with the same security settings.

Final Integration Testing tests all of the business application or infrastructure solution's access or touch points, across multiple business applications and systems, front to back (horizontal) and top to bottom (vertical), to ensure the solution works as required in a production-like environment. Final Integration Testing will be conducted on a complete, integrated set of business applications, infrastructure, and systems to evaluate whether the business applications, infrastructure, and systems interoperate correctly and pass data and control correctly to one another. This testing function is sometimes referred to as Volume Regression Testing, End-to-End Test, or End-to-End Integration Validation.

5.5 Initial Contingency Planning Testing

For new business applications or infrastructure, or for business applications or infrastructure with a major change, Initial Contingency Planning Testing must be done in accordance with the *CMS*

Policy for the Information Security Program before the business application or infrastructure moves into a production environment.

Initial Contingency Planning Testing will be performed as a tabletop test by personnel designated in a business application's or infrastructure's CP, to ensure the personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner.

6. Operational Testing

The business application and infrastructure Operational Testing functions will be performed to ensure that a business application or infrastructure solution is installed and configured correctly in a production environment, and that it behaves correctly once operational.

6.1 Production Ready Testing

The CMS IT Infrastructure Implementation Agent or Contractor will perform Production Ready Testing for a business application or infrastructure, with support provided by the testing contractor and the system developer/maintainer for a business application. Production Ready Testing is a regression test to confirm that a production-ready business application or infrastructure has been installed and configured correctly in a production environment and is ready for operational use.

If the business application requires data conversion, this testing function will include data conversion testing, as prescribed by the Data Conversion Plan.

6.2 Monitoring & Reliability Testing

The CMS IT Infrastructure Implementation Agent or Contractor will monitor the operational availability of business applications or infrastructure, problems/incidents, performance/service level, and capacity utilization of production systems, and will validate the gathered data against expected results to ensure that the implemented application or infrastructure performs as expected in production. Problems identified with a business application or infrastructure deployed to a production environment will be assessed to determine whether or not a rollback will be required to the previous production release. This testing function is sometimes referred to as Reliability Validation, Burn in Period, Reliability Test, or Extended Reliability Test.

6.3 Operational ST&E

An Operational ST&E will be performed by an IV&V or independent testing contractor every three (3) years for every business application or infrastructure operating in a production environment. Operational ST&E determines the extent to which the security controls in the business application or infrastructure are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the business application or infrastructure. Operational ST&E may include vulnerability scanning, penetration testing, and/or testing security standards and policy.

6.4 Audits

The CMS IT Infrastructure Implementation Agent or Contractor will perform audits to ensure a business application or infrastructure complies with prescribed auditing requirements and operating standards, and to assure accuracy of operating statistics and reporting, risk analysis,

information security, disaster recovery and contingency planning, corrective action planning, and quality assurance of all procedures.

6.5 Operational Contingency Planning Testing

Operational Contingency Planning Testing is performed as a tabletop test annually for systems operating in a production environment. Operational Contingency Planning Testing will be performed by personnel designated in a business application's or infrastructure's CP, to ensure the personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner.

Acronyms

BAMG	Business Applications Management Group
CAP	Corrective Action Plan
CCB	Configuration (or Change) Control Board
CIO	Chief Information Officer
CMS	Centers for Medicare & Medicaid Services
COTS	Commercial Off-the-Shelf
CP	Contingency Plan
CPU	Central Processing Unit
CR	Change Request
EASG	Enterprise Architecture and Strategy Group
EDCG	Enterprise Data Center Group
EDG	Enterprise Databases Group
EIT	Electronic Information Technology
ESD	Enterprise Systems Development
FISMA	Federal Information Security Management Act
GOTS	Government Off-the-Shelf
GTL	Government Task Leader
ICD	Interface Control Document
IRR	Implementation Readiness Review
ISDDG	Information Services Design and Development Group
IS RA	Information Security Risk Assessment
IT	Information Technology
IV&V	Independent Verification and Validation
FISMA	Federal Information Security Management Act
O&M	Operations and Maintenance
OIS	Office of Information Services
ORR	Operational Readiness Review
PBR	Project Baseline Review
PDR	Preliminary Design Review
PHI	Personal Health Information

PII	Personally Identifiable Information
PISP	Policy for Information Security Program
PPA	Project Process Agreement
PR	Problem Report
SDD	System Design Document
SOA	Service Oriented Architecture
SSP	System Security Plan
ST&E	Security Test and Evaluation
TIR	Test Incident Report
TRA	Technical Reference Architecture
TRB	Technical Review Board
VDD	Version Description Document
VRR	Validation Readiness Review