
Department of Health and Human Services


Centers for Medicare & Medicaid Services
Office of Information Services

# CMS Testing Framework Overview

Version 1.1

May 18, 2011

# Table of Contents

**1. Introduction ..... 1**

1.1 Purpose ..... 1
1.2 Scope ..... 1
1.3 Audience ..... 2
1.4 Document Organization ..... 2

**2. CMS Testing Framework Overview ..... 3**

2.1 Business Application Testing Overview ..... 4
2.2 Infrastructure Testing Overview ..... 7
2.3 Categories of Testing ..... 8
2.4 Deliverables ..... 10
2.5 Reviews ..... 11
2.6 Roles and Responsibilities ..... 13
2.7 Testing Tools ..... 15
2.8 Test Data ..... 15

**3. Development Testing ..... 16**

3.1 Unit Testing ..... 16
3.2 Application Integration Testing ..... 16
3.3 Section 508 Testing ..... 16

**4. Validation Testing ..... 17**

4.1 Business Application Validation Testing Functions ..... 17
4.1.1 System Testing ..... 17
4.1.2 Functional Testing ..... 17
4.1.3 End-to-End Integration Testing ..... 17
4.1.4 User Acceptance Testing ..... 18
4.1.5 Regression Testing ..... 18
4.1.6 Section 508 Testing ..... 18
4.2 Infrastructure Validation Testing Functions ..... 18
4.2.1 Infrastructure Testing ..... 18
4.2.2 Infrastructure Regression Testing ..... 19
4.2.3 Application Regression Testing ..... 19
4.2.4 Section 508 Testing ..... 19

**5. Implementation Testing ..... 20**

5.1 System Acceptance Testing ..... 20
5.2 Performance & Stress Testing ..... 20
5.3 Initial ST&E ..... 21
5.4 Final Integration Testing ..... 21
5.5 Initial Contingency Planning Testing ..... 22

**6. Operational Testing ..... 23**

6.1 Production Ready Testing ..... 23
6.2 Monitoring & Reliability Testing ..... 23
6.3 Operational ST&E ..... 23
6.4 Audits ..... 24
6.5 Operational Contingency Planning Testing ..... 24

**Acronyms ..... 25**

# List of Figures

Figure 1: Type of Figure: Testing Function per Environment ..... 6

# List of Tables

Table 2: Role of ILC Framework Deliverables in the CMS Testing Framework ..... 10
Table 3: Role of ILC Framework Reviews in the CMS Testing Framework ..... 12
Table 4: CMS Testing Framework Roles & Responsibilities ..... 13

# 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 "ILC 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 ILC Framework 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 ILC 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 ILC Framework phases of Development, Test, Implementation, and O&M. This document also identifies the various deliverables and reviews prescribed by the ILC Framework and their specific role in the CMS Testing Framework.

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, development, implementation, maintenance 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.

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 in the test plan, such as content, methodology, prioritization, and progression of testing activities.

For example, the project's testing methodology should 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 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). This does not preclude CMS from defining the deliverable and its format. 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 ILC Framework 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 (Annual Security Control Testing), 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

---

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.

- the three primary ILC 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 ILC 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.

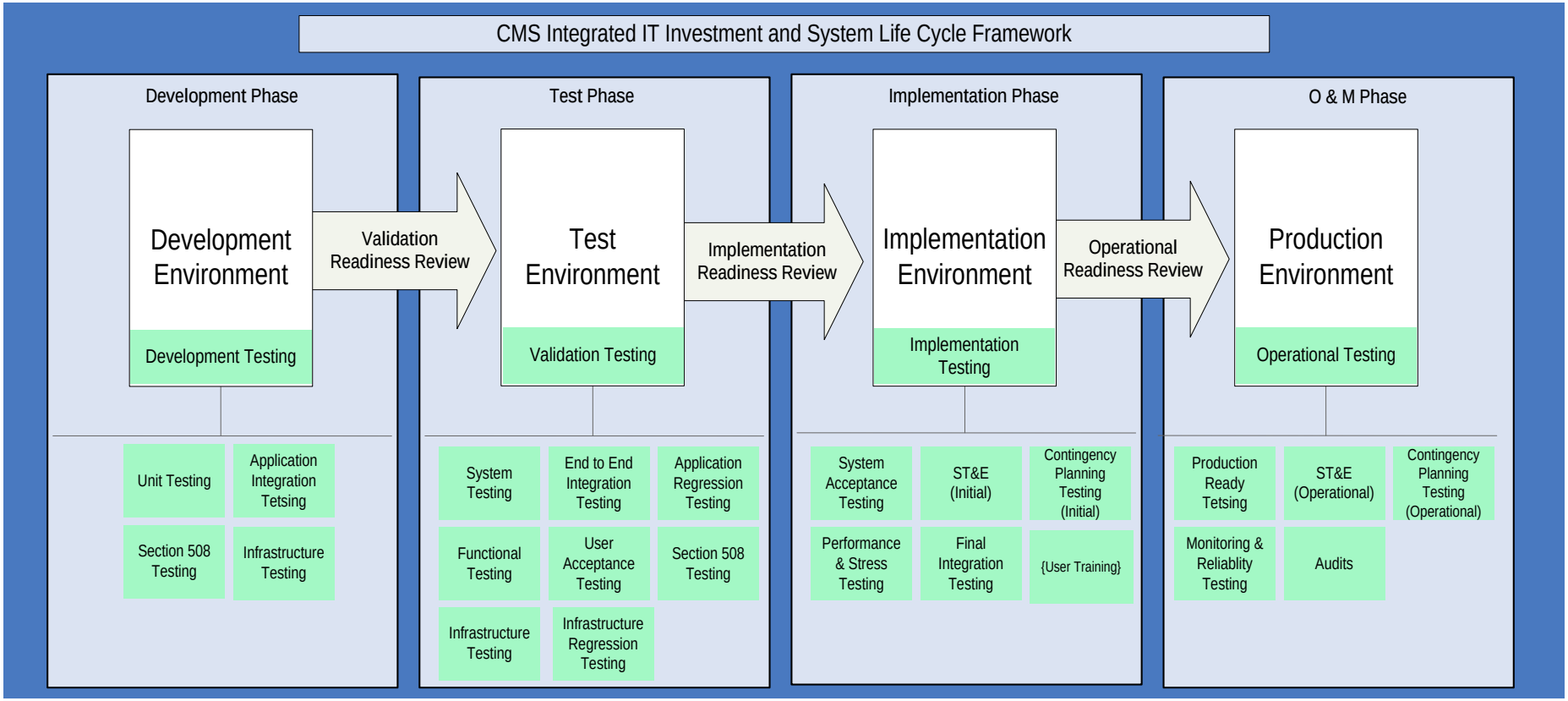


Figure 1: Type of Figure: Testing Function per Environment

## 2.2 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 ILC Framework 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 (Annual Security Control Testing), 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 ILC 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 ILC 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.

## 2.3 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.

- Dev site verses cms dev site.

  Development testing includes the business application testing functions of Unit Testing, Application Integration Testing, and Section 508 Testing. Infrastructure Testing should be performed as well.

- **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 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. Infrastructure Testing and Infrastructure Regression Testing should be take place as well.

- **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 (Annual Security Control Testing), Audits, and Operational Contingency Planning Testing.

## 2.4 Deliverables

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

**Table 2: Role of ILC Framework Deliverables in the CMS Testing Framework**

| Deliverable | Role in CMS Testing Framework |
|---|---|
| Business Product/Code | The primary object of the testing. |
| Change Request (CR) | Each CR should be properly tested throughout the various phases of its life cycle. |
| Contingency Plan (CP) | CMS CP tabletop testing is required to be done annually for CMS business applications. Contingency Plan testing for the infrastructure requires an annual functional CP test as defined by National Institute of Standards and Technology (NIST) SP 800-34. |
| Corrective Action Plan (CAP) | Used to track the status of a finding from the execution of the Initial or Operational ST&E testing functions. |
| Database Design Document | Used in test planning and in the generation of test data and test cases. |
| Data Conversion Plan | Used in test planning and the generation of test data and test cases. |
| Implementation Plan | Used as a reference in conducting Implementation Testing and Operational Testing. |
| Information Security Risk Assessment (IS RA) | Required for an ST&E and Certification & Accreditation. |
| Interface Control Document (ICD) | Used in test planning and in the generation of test data and test cases. |
| Operations and Maintenance (O&M) Manual | 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 testing. |
| Project Process Agreement (PPA) | 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 test-related tasks and milestones. |
| Release Plan | Determines the specific functionality to be tested based upon the functionality contained within a specific release. |

| Deliverable | Role in CMS Testing Framework |
|---|---|
| Requirements Document | Defines the requirements that are to be tested. |
| Section 508 Product Assessment | Used in test planning and the generation of test cases and test data. |
| System Design Document (SDD) | Used in test planning and in the creation of test data and test cases. |
| System Security Plan (SSP) | 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. More than one Test Plan may be prepared to address a specific testing function (Note: a separate ST&E Test Plan must be prepared and may be 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. |
| Test Summary Report(s) | Documents the results from the various tests performed. |
| Version Description Document (VDD) | The VDD provides a summary of the features and contents for a specific software build or release, and facilitates testing. Should 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 ILC Framework reviews, and other available guidance, as well as templates for these various deliverables are available from within the ILC 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 ILC Framework and their specific role in the CMS Testing Framework.

**Table 3: Role of ILC Framework Reviews in the CMS Testing Framework**

| Review | Role in CMS Testing Framework |
|---|---|
| Project Baseline Review (PBR) | 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. |
| Preliminary Design Review (PDR) | Ensures the testing strategy contained within the Test Plan is sufficient based upon the application's design. |
| Validation Readiness Review (VRR) | Conducted to ensure that the software has completed Development Testing and is ready for Validation Testing. |
| Implementation Readiness Review (IRR) | Conducted to ensure that the software has completed Validation Testing and is ready for Implementation Testing. |
| System Certification | ST&E results are a component of this evaluation. |
| System Accreditation | ST&E results are a component of this evaluation. |
| Operational Readiness Review (ORR) | Conducted to ensure that the software has completed Implementation Testing and is ready for Operational Testing. |
| Independent Verification & Validation (IV&V) Assessment | IV&V may be performed for any of the test-related activities, deliverables and/or processes. |

Detailed descriptions that further describe the purpose, audience, roles and responsibilities, related deliverables, and other available guidance are available from within the ILC 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 ILC 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 business requirements are met, which may be facilitated by a Testing Contractor. Certifies that the information system fully complies with Federal Information Security Management Act (FISMA) security requirements and ensures appropriate security measures and supporting documentation are maintained. Ensures other 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). |

| Role | Responsibilities in CMS Testing Framework |
|---|---|
| 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). |
| 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. |
| 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. In the case of ST&E, an independent entity, separate and apart form the development and maintenance, must perform the test. |
| 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, and ST&E. |

| Role | Responsibilities in CMS Testing Framework |
|---|---|
| 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. |
| Configuration (or Change) Control Board (CCB) | Approves changes for release into test, implementation and 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 and compare against the baseline. |

## 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*, which can be found on the CMS Intranet on the OIS Modernization page (http://cmsnet.cms.hhs.gov/hpages/oisnew/foffice/m/ITModern.asp)

## 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 of moderate sensitivity including 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., randomize the identifiers in 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. The results of the Validation 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 the Implementation Environment

## 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 documented 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. This can be done by comparing against the application's last baseline and/or threshold notes in the OM Documents.

### 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. The results of the Implementation 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 the Production Environment

## 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 and/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 and/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 as defined in the system's requirements document and/or Operation Manual (OM) document. 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 independent entity 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 must test all the applicable controls.

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 (IS) Assessment 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 business application Contingency Planning Testing will be performed as a tabletop test by personnel designated in a business application'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. Initial infrastructure Contingency Planning Testing will be performed as a functional test by personnel designated in the infrastructure's CP or Disaster Recovery Plan.

# 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, also known as Smoke Testing and Sanity 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.

## 6.2 Monitoring & Reliability Testing

The CMS IT Infrastructure Implementation Agent or Contractor will monitor the operational availability of business applications and/or infrastructure, problems/incidents, performance/service level, and capacity utilization of production systems, and will validate the gathered data against expected results (documented in the system's requirement document and/or Operation Manual (OM) document) 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 independent entity every three (3) years (or when there is a major change, change in security profile, or major security violation) 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.

Business Owners are required to test their security controls annually as part of their FISMA compliance. If the Business Owner uses an independent entity to test approximately 1/3 of their controls for this annual testing, they can meet the requirement for ST&E every three (3) years with these tests. However, if the annual testing requirement is performed in-house or by the system maintainer, all controls must be tested by an independent entity at the end of three (3) years.

## 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.

In addition, audits required by other legislation (e.g. A-123, CFO, FISMA, etc.) will be conducted for the purpose of validating compliance with these mandates to ensure that the proper financial and security controls have been implemented.

## 6.5 Operational Contingency Planning Testing

Operational Contingency Planning Testing for business applications 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 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. Operational Contingency Planning Testing for infrastructure will be performed as a functional test by personnel designated in the infrastructure's CP or Disaster Recovery Plan. This testing must be performed within 365 days of the last CP test.

# 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 of 2002 |
| **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 |
| **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 |