



Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS Policy for Software Quality Assurance

July 2002

Document Number: CMS-CIO-POL-QA001.1

TABLE OF CONTENTS

1. PURPOSE	1
2. BACKGROUND	1
3. SCOPE	1
4. POLICY	2
4.1. NOTICE OF PROJECT INITIATION AND SYSTEM RELEASE–INTERNAL SYSTEMS	2
4.2. SOFTWARE CONFIGURATION MANAGEMENT AND VALIDATION TESTING	2
4.3. PRODUCTION CONTROL	3
4.4. WAIVERS	3
5. ROLES AND RESPONSIBILITIES	4
5.1. CHIEF INFORMATION OFFICER (CIO)	4
5.2. CIO PLANNING, MANAGEMENT, AND SUPPORT GROUP (PMSG)	4
5.3. SYSTEM DEVELOPERS/MAINTAINERS AND BUSINESS OWNERS/PARTNERS	4
5.4. MANAGERS OF SYSTEM DEVELOPERS/MAINTAINERS AND BUSINESS OWNERS/ PARTNERS	4
6. APPLICABLE LAWS/GUIDANCE	4
7. EFFECTIVE DATES	5
8. INFORMATION AND ASSISTANCE	5
9. APPROVED	5
10. GLOSSARY	5

1. PURPOSE

This document establishes CMS's policy for software quality assurance (SQA).

SQA includes:

- Notice of Project Initiation and Software Release
- Software Configuration Management
- Validation Testing
- Waivers
- Reviews

2. BACKGROUND

Standardized software quality assurance policies are an integral part of CMS's systems development life cycle (SDLC). Sound quality assurance processes have been found to reduce the number of errors and the cost of rework associated with new systems. CMS released an "Interim Quality Assurance Policy for Internal Systems" in April 2000, as an initial step to standardizing its SQA policies.

In March 2000, CMS's *Software Process Improvement (SPI) Program Plan* established four SPI goals, the fourth of which is to achieve "the software engineering and project management capability defined in SW-CMM Maturity Level 2". In addition, in its *HHS IRM Guidelines for Capital Planning and Investment Control* (January 2001), the Department of Health and Human Services (DHHS) urged its operating divisions "To fully implement the Clinger-Cohen Act, ... to strive, at a minimum, to meet the Software Engineering Institute (SEI) Capability Maturity Model (CMM) level 2, the repeatable level". SCM and SQA are two of the six "key process areas" for assessing Level 2 maturity.

In July 2000, the CMS IT Council adopted Institute of Electrical and Electronics Engineers (IEEE) Standard 12207, Software life cycle processes, as the CMS SDLC, in the context of the IEEE's four-volume set, *Software Engineering, 1999 Edition*. IEEE Standard 12207 requires SCM and SQA as "supporting processes."

3. SCOPE

This policy applies to all IT activities and IT assets owned, leased, controlled or used by CMS, including those of CMS's agents, contractors or other business partners when acquired or supported by CMS funding. As such, the policy applies to both internal and external systems—unless otherwise specified.

4. POLICY

This policy supercedes the “Interim Quality Assurance Policy for Internal Systems” released April 11, 2000, as well as any other policies on these subjects. Detailed instructions are found in the separately published implementation procedures.

The policy mandates compliance with the following series of requirements:

4.1. Notice of Project Initiation and System Release–INTERNAL SYSTEMS

System developers/maintainers or business owner(s)/partner(s) for CMS internal systems shall provide notification twice during the life cycle of each project in order to plan for quality assurance support that may be appropriate for the project.

- 4.1.1 Project Initiation. System developers/maintainers or business owner(s)/partner(s) shall provide notification of the initiation of new systems development projects or of modification(s) to existing systems.

In addition to the notification, for those projects approved by the Financial Management Investment Board (FMIB) that require a business case analysis (BCA), a briefing shall be provided to the Project Review and Coordination Panel (PRCP) after the BCA is complete, in accordance with the IT Investment Management Policy.

For in-house projects (projects being done with CMS internal resources only) involving the development of new systems, the system developer/maintainer and business owner(s)/partner(s) shall provide an abbreviated BCA to the PRCP for review prior to the PRCP briefing.

- 4.1.2. System Release. When any system release is being prepared for placement in a CMS production run library, the system developer/maintainer and business owner(s)/partner(s) shall provide notice of the proposed system release.

4.2. Software Configuration Management and Validation Testing

All CMS systems shall be maintained using SCM. Acceptable SCM shall address all of the following criteria.

- 4.2.1. Use of a configuration management tool to provide at least version control of all source code;
- 4.2.2. Use of a change management process; and
- 4.2.3. Completion of validation testing prior to release of the system for production use.

4.2.4. There are two mandatory reviews.

4.2.4.1. Prior to validation testing a validation readiness review shall occur.

4.2.4.2. Prior to system implementation an implementation readiness review shall occur.

For internal systems, system developers/maintainers shall follow specific procedures that have been developed to comply with these requirements.

4.3. Production Control

All CMS systems shall be released to and run under an appropriate production control environment, following production control procedures available within the platform(s) used.

4.4. Waivers

All CMS Internal Systems will use products that comply with CMS standards, as recorded in the CMS Technical Reference Model, or appropriately justify a waiver. If deemed necessary, justification for deviation(s) or waiver(s) will be supplied for evaluation through the IT standards/products review process. Any approved waivers to such standards and preferred products will, at minimum, require that the non-standard implementation fully interoperate and intercommunicate with standard implementation(s).

For additional guidance regarding topics related to SQA and SCM, please refer to:

Subject Area	Resource	URL
A list of the standard CMS automated SCM tools	CMS Technical Reference Model	http://hcfanet.hcfa.gov/hpages/ois/ita2000/architectrmpop.pdf
IT standards/products review process	CMS IT Policy Management Policy	[to be published]
IT Investment Management Policy		http://hcfanet.hcfa.gov/roadmap/phases/Investment_Mgmt_Policy.pdf

5. ROLES AND RESPONSIBILITIES

The following entities have responsibilities related to the implementation of this policy:

5.1. Chief Information Officer (CIO)

The CIO shall mandate adherence to this policy.

5.2. CIO Planning, Management, and Support Group (PMSG)

PMSG shall:

- Disseminate this policy to all CMS components.
- Maintain the content of this policy.
- Monitor adherence to this policy and report status to the CIO.
- Facilitate implementation of this policy, including providing the training needed for adherence to this policy.
- Assign a quality assurance point of contact (QA POC) for each CMS system.

5.3. System Developers/Maintainers and Business Owners/Partners

Developers, maintainers and business owners will:

- Adhere to this policy.
- Provide project initiation and release notices to Division of Investment Support (DIS), PMSG.
- Participate in validation readiness reviews, validation testing, and implementation readiness reviews.

5.4. Managers of System Developers/Maintainers and Business Owners/Partners

Managers will approve project initiation and system release notices.

6. APPLICABLE LAWS/GUIDANCE

The following laws and guidance are applicable to this Policy:

- 6.1 Information Technology Reform (Clinger-Cohen) Act of 1996, also known as the Chief Information Officers Act, especially sections 5122(b)(6) and 5123(4).
- 6.2 IEEE/EIA Standard 12207.0-1996, *Software life cycle processes*, March 1998.

- 6.3. *HHS IRM Guidelines for Capital Planning and Investment Control*, HHS-IRM-2000-0001-GD, January 8, 2001, especially G. Guideline, G: The Capability Maturity Model.
- 6.4. *Draft Strategic Plan*, Revised March 21, 2002, Operational Objectives: Program Administration 2, Modernize and effectively manage CMS' information systems and technology.
- 6.5. *HCFA Software Process Improvement (SPI) Program Plan*, February 10, 2000.

7. EFFECTIVE DATES

This policy will take effect May 2002.

This policy remains in effect until formally cancelled or superseded by the CIO.

8. INFORMATION AND ASSISTANCE

The CMS organization responsible for maintaining the content of this policy is Division of Investment Support (DIS), CIO Planning, Management, and Support Group (PMSG), Office of Information Services. The people able to speak knowledgeably about the content of this policy are Ann Pollock, DIS Director, 410-786-6405 and Bruce Tarantino, DIS Deputy Director, 410-786-5140. Questions may also be sent to the GroupWise resource "SQA Policy Questions".

9. APPROVED

_____/s/_____
Timothy P. Love
Acting Chief Information Officer

_____/5/31/2002_____
Date of Issuance

10. GLOSSARY

This alphabetically sequenced section defines terms used in this policy, such as:

Business owners/partners – The entity or entities responsible for defining, promoting, endorsing, and upholding the business needs and user requirements for the system, and for performing user acceptance testing of the final product(s) based on those business needs and user requirements. The business owners/partners define and validate system functionality, access rights, business rules, and the privacy classification, timeliness, completeness, and accuracy of data.

CMM – The capability maturity model developed by the SEI.

Configuration item (CI) – “An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration process.” (IEEE Std. 610-12-1990)

Configuration management (CM) – “A discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements.” (IEEE Std. 610-12-1990)

Implementation readiness review (IRR) – A formal review that ensures that all prerequisites for implementation to production have been met.

Internal system – A CMS internal system is one that that will be developed within, released from, or run primarily within CMS production-controlled infrastructure, or that is developed outside of these parameters, but is expected to eventually be run primarily within CMS production-controlled infrastructure.

Level 2 – The maturity level of the CMM at which an organization’s requirements management, project planning, project tracking and oversight, subcontract management, quality assurance, and configuration management processes have become “repeatable.”

Quality assurance (QA) – “(1) A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. (2) A set of activities designed to evaluate the process by which products are developed or manufactured.” (IEEE Std. 610-12-1990)

SEI – The Software Engineering Institute, developer of the CMM.

System developer - The system developer is an individual or a group of individuals from within CMS, another Federal agency and/or a contractor who have the responsibility for the development, testing, and implementation of a system based upon its documented requirements and certified information technology architecture. A system developer may or may not also serve as the system maintainer for a given project.

System maintainer - The system maintainer is an individual or a group of individuals from within CMS, another Federal agency and/or a contractor who have the responsibility for continued maintenance (e.g., bug fixing, minor modifications/enhancements, performance tuning, and/or customer service) of an implemented system. A system maintainer may or may not also serve as the system developer for a given project.

Validation – “The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.” (IEEE Std. 610-12-1990)

Validation readiness review (VRR) - A formal review that ensures that all prerequisites have been met and environmental preparations have been completed prior to commencement of validation testing.

Validation testing – Validation testing is considered the final phase of testing and is performed just prior to releasing a new or changed system into production. This may be separate testing or “system testing” or “user acceptance testing” may double as the validation testing required by this policy. The scope of testing will depend on the extent of changes involved (e.g., major revisions to a system would warrant that full system testing be conducted).

Version – “(1) An initial release or re-release of a computer software configuration item, associated with a complete compilation or recompilation of the computer software configuration item. (2) An initial release or complete re-release of a document, as opposed to a revision resulting from issuing change pages to a previous release.” (IEEE Std. 610-12-1990)

Version Control – The process of managing configuration items (e.g., source files).