

**Information Technology Architecture
Conformance Certification Criteria
Guide**

Version 2.3

Revised September 2002

Prepared by:

Office of Information Services
CIO Planning, Management, and Support Group
Division of Architecture and Strategic Planning

Table of Contents

- I. Introduction..... 1**
- II. General Criteria..... 1**
 - Table 1 - General Conformance Criteria..... 2
- III. Specific Criteria 5**
 - Table 2 - Specific Conformance Criteria..... 5
- IV. Assumptions 8**
- V. Glossary of Terms 10**

I. Introduction

This document contains criteria intended for use as guidelines in developing information systems and for use in reviewing IT projects for conformance with CMS's Information Technology Architecture (ITA). A primary purpose of the ITA is to provide guidance that advances systems development towards a future state environment as described in CMS's IT Vision and eight IT Objectives. Both the IT Vision and IT Objectives are contained in ITA Volume 1.

General criteria and specific criteria are proposed. The general criteria apply across multiple domains of the ITA (i.e., Business, Information, Application, Infrastructure, and Security). Specific criteria apply to the particular ITA domain as indicated.

Each criterion is defined as either Mandatory or Preferred based upon the following considerations:

- Mandatory criteria are established for achieving system design and development outcomes that are consistent with documented standards, policies, and design guidance. CMS's system development processes exist to enable all IT development projects to meet expectations as described.
- Preferred criteria are established as "best practices" that help to achieve CMS's IT Objectives by promoting particular system design and development outcomes. IT projects should incorporate these criteria where practical and feasible, without compromising a project's success.

IT system development projects must satisfy the Mandatory criteria in order to be in conformance with the ITA. Preferred criteria are optional, but strongly encouraged.

II. General Criteria

- A. ITA Volume 1, IT Direction, lists 15 IT Guiding Principles that provide broad guidance for evolving CMS's IT environment from the current to a future state as described in the eight IT Objectives. Guiding Principles 1 through 4 and 15 apply to the management and governance of CMS's IT environment. They are not directly applicable to individual IT projects. Guiding Principles 5 through 14, however, apply directly to IT projects.
- B. IT projects should adhere to Guiding Principles 5 through 14 as presented in Table 1 to the extent possible. Project Owners/Managers should provide explicit language in IT Fact Sheets, Statements of Work, or appropriate systems development documentation describing how each principle will be satisfied. Quantifiable evidence should be presented to substantiate the project's effort. Unsubstantiated statements alone are unsatisfactory. It may be impractical for any given project to embrace all the principles

Information Technology Architecture Conformance Certification Criteria Guide

simultaneously; however, projects should make reasonable effort to do so. Projects should provide a written justification for any principle that cannot be satisfied, and avoid actions that foreclose the ability to satisfy principles at a later stage, should conditions become favorable.

- C. CMS’s technology policy encourages using *Target* technology standards and products for Enterprise applications¹. Enterprise applications use *Interim* standards and products only where a *Target* does not exist, or its use is infeasible. A waiver may be requested by the Project Owner/Manager, justifying the use of technology standards and products from other categories, and submitted through the IT Investment Technical Review Process¹ for approval. (Note: Acceptable technology standards and products are listed in ITA Volume 5, Infrastructure Architecture, Attachment B, and in the IT Standards Profile database, which is accessible via the Roadmap Web site on the CMSNet).

- D. Guiding Principles are more general and may be augmented by specific guidance in Table 2. In these instances, the specific guidance should also be satisfied.

Table 1 - General Conformance Criteria

General Conformance Criteria		Expectations
Reference: ITA Volume 1 – IT Direction		
1. Guiding Principle 5: Develop and Implement IT Projects Using Enterprise-Wide Methodologies (<i>Preferred</i>)	<ul style="list-style-type: none"> a) Methods approved for enterprise-wide adoption are utilized. b) Documentation of the system development methodology is provided. c) Project deliverables that conform to the methodology are available as evidence. 	
2. Guiding Principle 6: Adopt Open System Standards (<i>Preferred</i>)	<ul style="list-style-type: none"> a) Standards defined in the ITA standards profile are used to the extent possible. b) Proprietary standards are used only in cases where no alternatives exist. 	
3. Guiding Principle 7: Enable Automated, Active Delivery of Information Across the Enterprise (<i>Preferred</i>)	<ul style="list-style-type: none"> a) Information sources are predefined and readily accessible. b) Publish and subscribe techniques are implemented to pre-register authorized users to receive requested information c) Information users are automatically notified of available information, which is delivered upon request. 	

¹ See ITA Volume 7, Management and Governance for more details about the IT Investment Technical Review Process.

Information Technology Architecture Conformance Certification Criteria Guide

General Conformance Criteria	Expectations
4. Guiding Principle 8: Manage Information and Data as Enterprise-Wide Assets (<i>Preferred</i>)	<ul style="list-style-type: none"> a) Data and information subject areas are classified based upon CMS's Information Model. b) Data stores are defined based upon CMS's enterprise Data Model. c) Security and privacy rules are defined.
5. Guiding Principle 9: Design and Develop Application Software Components for Reusability and Platform Independence (<i>Mandatory</i>)	<ul style="list-style-type: none"> a) Common business system services are defined as discrete modules that are reusable in multiple systems. b) Business applications are designed and developed as discrete modules that perform logical units of work. c) Business application modules are developed using languages that are portable across platforms where feasible and practical. d) Business applications use standard interfaces between loosely coupled modules.
6. Guiding Principle 10: Use Custom-Developed Software Instead of Commercial/Government Off-the-Shelf Products Only When Warranted and Justified (<i>Mandatory</i>)	<ul style="list-style-type: none"> a) Information systems use commercial off-the-shelf (COTS) or government off-the-shelf (GOTS) software instead of custom-designed solutions. b) Custom-developed solutions are used only where warranted and justified. c) COTS and GOTS product customization to meet business needs is avoided.
7. Guiding Principle 11: Leverage Enterprise-Wide Licensing of Vendor Products (<i>Mandatory</i>)	<p>To leverage CMS' buying power, technology is procured through negotiated enterprise licenses when appropriate. This approach provides cost savings over component-specific licensing.</p>
8. Guiding Principle 12: Promote the Use of Web-Based Technology (<i>Preferred</i>)	<ul style="list-style-type: none"> a) Web browsers are used for application user interfaces, rather than custom interfaces. b) Internet-based standards are used for network connectivity, distributed processing, security, data sharing and access.
9. Guiding Principle 13: Design and Deploy Application Systems Using a Client/Server Model (<i>Mandatory</i>)	<ul style="list-style-type: none"> a) Business application modules are designed and developed in logical layers that perform defined services. b) Business application services can be deployed onto a distributed computing infrastructure.

General Conformance Criteria	Expectations
10. Guiding Principle 14: Ensure Enterprise-Wide Integration of IT Security (<i>Preferred</i>)	<ul style="list-style-type: none"> a) Enterprise-wide security policies and services are defined. b) Enterprise-wide user roles are defined and utilized to control application system and data access privileges. c) Common, reusable security services are utilized.

III. Specific Criteria

Specific conformance criteria provided in Table 2 pertain to each ITA domain. Refer to the associated ITA volume for specifics pertaining to each of the domain architectures.

Table 2 - Specific Conformance Criteria

Specific Conformance Criteria	Expectations
Reference: ITA Volume 2 - Business Architecture	
11. Link business process requirements, decompositions, and descriptions to the enterprise Business Function Model (BFM) (<i>Mandatory</i>)	<ul style="list-style-type: none"> a) IT projects should identify the CMS business functions and processes that are affected. b) Project Owners/Managers provide specific language in their IT Fact Sheets and in appropriate systems development documentation that describe the relationships and interactions between the business functions and processes that are affected.
12. Use acceptable standard formats for business models (<i>Preferred</i>)	<ul style="list-style-type: none"> a) IT projects should provide models of pertinent business functions using published CMS standards. b) The models are consistent with the business function model framework provided in ITA Volume 2. c) The project-specific models that modify, extend, or further decompose the ITA Business Function Model (BFM) have been coordinated and properly mapped to the enterprise BFM.

Information Technology Architecture Conformance Certification Criteria Guide

Specific Conformance Criteria	Expectations
Reference: ITA Volume 3 - Information Architecture	
13. Information - Design Principle 1: Use basic mission/business activities to guide the building of data and information topic structures <i>(Mandatory)</i>	Data models are designed to be consistent with CMS's enterprise models (Information Model and enterprise Data Model).
14. Information - Design Principle 2: Establish Metadata store(s) as a decision support and operational tool <i>(Mandatory)</i>	Both business and technical Metadata are captured and accessible.
15. Information - Design Principle 3: Separate transaction processing and analytical support data stores <i>(Mandatory)</i>	Databases used for online or batch transaction processing should not be directly accessed for decision support.
16. Information - Design Principle 4: Plan for supporting data in a distributed environment <i>(Mandatory)</i>	An information system's design considers access of both data and Metadata stores by geographically distributed customers.
17. Information - Design Principle 5: Minimize the data collection burden <i>(Mandatory)</i>	A project / information system collects only those data elements required to support a specific business need.
18. Information - Design Principle 6: Address issues of document interoperability <i>(Mandatory)</i>	An information system's design considers access to key electronic documents, and integration of access to those documents (or information about those documents) as a complement to data access.
19. Information - Design Principle 7: Support Records Management requirements <i>(Mandatory)</i>	An information system's design considers retention and archival requirements for both data and documents.
Reference: ITA Volume 4 - Application Architecture	
20. Application - Design Principle 1: Design Applications to Mimic a Business Process <i>(Mandatory)</i>	The physical design boundaries of an application process (starting and ending points) are discrete and distinct to the business process it supports.
21. Application – Design Principle 2: Layer the Design of Applications <i>(Mandatory)</i>	<ul style="list-style-type: none"> a) Logical and physical separations are maintained (loosely coupled) between the user interface (presentation), business logic, and data access modules of a business application. b) Loosely coupled modules communicate with each other using messaging services (see Design Principle 3).

Specific Conformance Criteria	Expectations
<p>22. Application - Design Principle 3: Use Standardized Messaging between Layers (<i>Mandatory</i>)</p>	<p>a) Loosely coupled modules communicate with each other using standardized messaging services (see Design Principle 2) to maintain logical and physical separations between the user interface (presentation), business logic, and data access modules of a business application.</p> <p>b) Standardized messaging services specified in the Technical Reference Model will be used.</p>
<p>23. Application - Design Principle 4: Design for Security Up Front (<i>Mandatory</i>)</p>	<p>a) Appropriate security services are included in the initial design specifications for business application systems.</p> <p>b) Until the ITA Security Architecture is completed, security design implementations may be project specific and limited to design constraints of the current technical infrastructure.</p>
<p>24. Application - Design Principle 5: Design Applications for Reuse (<i>Mandatory</i>)</p>	<p>Same as Guiding Principle 9, see General Criterion #5, as follows:</p> <ul style="list-style-type: none"> • Common business system services are defined as discrete modules that are reusable in multiple systems. • Business applications are designed and developed as discrete modules that perform logical units of work. • Business application modules are developed using languages that are portable across platforms where feasible and practical. • Business applications use standard interfaces between loosely coupled modules.
<p>25. Application - Design Principle 6: Design Applications for Portability and Platform Independence (<i>Mandatory</i>)</p>	<p>Where feasible and practical in distributed systems, business application modules are developed using languages that are portable from one operating system platform to another so as to minimize redesign, re-coding, and redundant maintenance.</p>
<p>26. Application - Design Principle 7: Use COTS/GOTS (<i>Mandatory</i>)</p>	<p>Same as Guiding Principle 10, see General Criterion #6 as follows:</p> <ul style="list-style-type: none"> • Information systems use commercial off-the-shelf (COTS) or government off-the-shelf (GOTS) software instead of custom-designed solutions. • Custom-developed solutions are used only where warranted and justified. • COTS and GOTS product customization to meet business needs is avoided.

Information Technology Architecture Conformance Certification Criteria Guide

Specific Conformance Criteria	Expectations
27. Application - Design Principle 8: Promote the Use of Web-based Technology (<i>Mandatory</i>)	Same as Guiding Principle 12, see General Criterion #8 as follows: <ul style="list-style-type: none"> • Web browsers are used for application user interfaces, rather than custom interfaces. • Internet-based standards are used for network connectivity, distributed processing, security, data sharing and access.
28. Application - Design Principle 9: Enable Automated, Active Information Delivery Technology (<i>Preferred</i>)	Data analysis and decision support systems are designed using "publish and subscribe" information delivery techniques, thereby minimizing the need for ad hoc user query.
29. Application - Design Principle 10: Separate OLTP from OLAP (<i>Mandatory</i>)	<p>a) Business applications that perform online transaction processing (OLTP) are implemented as separate application processes from those that perform online analytical processing (OLAP).</p> <p>b) OLTP processes may be provided using COTS products, custom-developed software, or a combined, integrated solution. OLAP solutions are provided using COTS products.</p>
30. Application - Design Principle 11: Design OLAP to use Data Warehousing (<i>Mandatory</i>)	<p>a) Business applications that perform online analytical processing (OLAP) are consistent with a data warehouse methodology to integrate with the enterprise-wide data warehousing strategy.</p> <p>b) OLAP applications will access a subject area data mart.</p>
31. Application - Design Principle 12: Design for N-Tier Client/Server (<i>Mandatory</i>)	Business applications use a multi-tiered client/server approach that permits flexibility in deploying logical layers of the system (see Guiding Principle 2) onto the enterprise infrastructure in an optimal manner.
32. Application - Design Principle 13: Use Standard Methods (<i>Mandatory</i>)	Business applications are produced using standard design techniques, development languages, COTS products, and standard deployment infrastructure.
33. Application - Design Principle 14: Use Prototypes and Pilots (<i>Mandatory</i>)	Business applications use prototypes to prove new design concepts and/or pilots to explore the viability of new technical solutions before full-scale investments are made in development efforts.

Specific Conformance Criteria	Expectations
Reference: ITA Volume 5 - Infrastructure Architecture	
34. Use infrastructure products that are registered in the ITA standards database (<i>Mandatory</i>)	Enterprise-level and departmental applications ² intended for deployment onto government-owned infrastructure use technology standards and products consistent with the policy and standards categories described in Section 5.4 of ITA Volume 5. Acceptable standards and products are listed in ITA Volume 5, Attachment B, and in the ITA Technical Reference Model (TRM) ³ , which is accessible via the Roadmap Web site.
35. Ensure that externally deployed systems conform to infrastructure interface standards (<i>Mandatory</i>)	Interfaces between non-government-hosted and government-hosted applications will adhere to interface policies specified in the External Environment Major Service Area (MSA) of the ITA Technical Reference Model (TRM).
Reference: ITA Volume 6 - Security Architecture	
36. Explicitly define security services within system design documentation (<i>Mandatory</i>)	Security services are implemented for each of the logical layers of a business application system consistent with CMS security policy and with services defined within ITA Volume 6.
37. Implemented security services in accordance with standards (<i>Preferred</i>)	Business application systems intended for deployment onto CMS-owned ⁴ infrastructure use security technology standards that are defined in ITA Volume 5, Attachment B, or in the IT Standards Profile database that is accessible via the Roadmap Web site.

IV. Assumptions

The following assumptions underpin these criteria:

- A. Users of these criteria are assumed to have an understanding of the ITA and to have access to its documentation. CMS IT Project Owners/Managers should use these criteria for planning their IT projects, and for self-assessing their project's conformance with the ITA. CMS staff involved in IT project

² See Glossary.

³ See ITA Volume 5, Infrastructure Architecture, Section 5.5.9 for descriptions of the TRM and MSA.

⁴ "CMS-owned" refers to any compute platform that is funded by CMS, whether government-owned or contractor owned, to host applications and process data to support CMS program operations.

Information Technology Architecture Conformance Certification Criteria Guide

investment review activities should use these criteria in evaluating the conformance of IT projects with the ITA.

- B. Throughout fiscal year 2002, significant changes will occur within CMS's IT environment, including:
 - 1. Roles, responsibilities, policies, and support for systems development and delivery within the Office of Information Services (OIS) will evolve;
 - 2. CMS's systems development life cycle (SDLC) methods and practices will be reshaped through the CMS Integrated IT Investment Management Roadmap development effort;
 - 3. CMS IT investment management processes are migrating to an incremental funding approach⁵;
 - 4. CMS's ITA and related processes will continue to mature and be integrated with other key IT management practices.
- C. Additional time will be needed for many of the activities listed above to achieve satisfactory levels of maturity such that they fully enable IT project delivery. Strict application of any conformance criteria within such a dynamic environment is impractical when reviewing IT projects that are dependent upon these activities for project completion. These factors argue the necessity for independent reviewers of IT projects to be balanced in their assessments.
- D. Technical assessments using the Guiding Principles as criteria are qualitative judgements, which are inherently subjective. Self-assessments performed by Project Owners/Managers, therefore, must be able to withstand reasonable scrutiny. When IT projects are reviewed through the IT Investment Technical Review Process, discretionary issues should yield benefit of doubt to the project.
- E. These criteria will evolve with the further development and integration of the ITA with other IT governance processes.

⁵ See the *IT Investment Management Process Guide*, August 2002, CIO Planning, Management, and Support Group, Office of Information Services, Centers for Medicare & Medicaid Services.

V. Glossary of Terms

Business application	One or more software programs that automate processes as defined within CMS's Business Function Model (BFM).
Business Function Model (BFM)	A logical model of CMS's business processes, including those related to information systems, as depicted and described in ITA Volume 2, Business Architecture.
Departmental application	Any business application that supports the operation of a single organizational group, division, or individual.
Enterprise application	Any major information system or business application that supports the operation of two or more formal organizational groups within CMS.
Information system	A logical or physical collection of related business applications that perform operations against a common database subject area as defined in ITA Volume 3, Information Architecture.