

## **Appendix G**

# **A Comparison of ISO 9001 and the Capability Maturity Model**

# Content

<b>G.1 Introduction</b> .....	<b>G-3</b>
G.1.1 Mapping Specifics .....	<b>G-3</b>
G.1.1.1 Clause 4.1: Management Responsibility .....	G-4
G.1.1.2 Clause 4.2: Quality System .....	G-4
G.1.1.3 Clause 4.3: Contract Review .....	G-5
G.1.1.4 Clause 4.4: Design Control .....	G-7
G.1.1.5 Clause 4.5: Document and Data Control .....	G-9
G.1.1.6 Clause 4.6: Purchasing .....	G-9
G.1.1.7 Clause 4.7: Control of Customer-Supplied Product .....	G-9
G.1.1.8 Clause 4.8: Product Identification and Traceability .....	G-10
G.1.1.9 Clause 4.9: Process Control.....	G-10
G.1.1.10 Clause 4.10: Inspection and Testing .....	G-10
G.1.1.11 Clause 4.11: Control of Inspection, Measuring, and Test Equipment.....	G-10
G.1.1.12 Clause 4.12: Inspection and Test Status .....	G-10
G.1.1.13 Clause 4.13: Control of Nonconforming Product .....	G-11
G.1.1.14 Clause 4.14: Corrective and Preventive Action .....	G-11
G.1.1.15 Clause 4.15: Handling, Storage, Packaging, Preservation, and Delivery .....	G-11
G.1.1.16 Clause 4.16: Control of Quality Records .....	G-12
G.1.1.17 Clause 4.17: Internal Quality Audits .....	G-12
G.1.1.18 Clause 4.18: Training .....	G-12
G.1.1.19 Clause 4.19: Servicing .....	G-12
G.1.1.20 Clause 4.20: Statistical Techniques .....	G-12
G.1.2 Summary .....	<b>G-13</b>
G.1.3 Compliance Issues .....	<b>G-14</b>
<b>G.2 Acknowledgements</b> .....	<b>G-16</b>
<b>G.3 References</b> .....	<b>G-16</b>
<b>G.4 Biography</b> .....	<b>G-16</b>

**Note: This appendix was extracted from the CMU/SEI-94-TR-12. You may view the entire document at <http://www.sei.cmu.edu>**

---

## G.1 Introduction

The Capability Maturity Model Model for Software, developed by the Software Engineering Institute, and the ISO 9000 series of standards, developed by the International Organization for Standardization, have the common concern of quality and process management. The two are driven by similar issues and are intuitively correlated, but they differ in their underlying philosophies: ISO 9001, the standard in the 9000 series that pertains to software development and maintenance, identifies the minimal requirements for a quality system, while the CMM underlines the need for continuous process improvement. This statement is somewhat subjective, of course; some members of the international standards community maintain that if you read ISO 9001 with insight, it *does* address continuous process improvement. Corrective action, for example, can be construed as continuous improvement. Nonetheless, the CMM tends to address the issue of continuous process improvement more explicitly than ISO 9001.

This article examines how the two documents relate. I have essentially mapped clauses of ISO 9001 to CMM key practices. The mapping is based on an analysis of ISO 9001, ISO 9000-3, TickIt (a British guide to using ISO 9000-3 and 9001), and the TickIt training manuals.<sup>1</sup> ISO 9000-3 elaborates the TickIt training materials help in interpreting both ISO 9000-3 and ISO 9001.

As part of the analysis, I attempt to answer some frequently asked questions, including

- At what level in the CMM would an ISO 9001-compliant organization be?
- Can a level 2 (or 3) organization be considered compliant with ISO 9001?
- Should my software-quality-management and process-improvement efforts be based on ISO 9001 or on the CMM?

I assume the reader is familiar with or has ready access to both ISO 9001 and the CMM. For those who need are fresher, the box on page G-6 gives an overview.

---

### G.1.1 Mapping Specifics

My analysis involved mapping ISO 9001's 20 clauses to CMM key practices at the sentence to subpractice level.<sup>2,3</sup> The analysis is admittedly subjective — others may interpret both ISO 9001 and the CMM differently (indeed, reliable and consistent interpretation and assessment are common challenges for CMM-based appraisals and ISO 9001 certification) — but hopefully there is enough objectivity to make the analysis worthwhile to those who wonder where ISO 9001 certification fits into a continuous quality-improvement strategy.

Table 1 (on page G-8) is an overview of the mapping from ISO 9001 clause to CMM key process areas and key practices. The column labeled “Strong relationship” contains key process areas and common features for which the relationship is relatively straightforward. The column labeled “Judgmental relationship” contains key process areas and common features that may require a significant degree of subjectivity in determining a reasonable relationship. Table A in the box on

page G-7 describes the focus of the key process areas and common features. In the Activities Performed common feature, key practices focus on systematically implementing a process, while the key practices in other common features focus on institutionalizing it.

### **G.1.1.1 Clause 4.1: Management Responsibility**

ISO 9001 requires an organization to

- define, document, understand, implement, and maintain a quality policy;
- define responsibility and authority for personnel who manage, perform, and verify work affecting quality; and
- identify and provide verification resources.

A designated manager ensures that the quality program is implemented and maintained. The CMM addresses responsibility for quality policy and verification at level 2. This includes identifying responsibility for performing all project roles, establishing a trained software quality assurance group, and assigning senior management oversight of SQA activities.

As practices within common features, the CMM identifies management's responsibility at both the senior- and project-management levels to oversee the software project, support SQA audits, provide leadership, establish organizational structures to support software engineering, and allocate resources.

You could argue that this clause also addresses the quality policy described at level 4, but the level 4 quality policy is quantitative. ISO 9001 is somewhat ambiguous about the role of measurement in the quality-management system (see discussion under "Clause 4.20: Statistical techniques"); an organization is required to define and document quality objectives, but it does not have to quantify them.

### **G.1.1.2 Clause 4.2: Quality System**

ISO 9001 requires an organization to establish a documented quality system, including a quality manual and plans, procedures, and instructions. ISO 9000-3 characterizes this quality system as an integrated process throughout the life cycle.

The CMM addresses quality-system activities for verifying compliance and for management processes at level 2. The specific procedures and standards a software project would use are specified in the software-development plan. At level 3, the organization must have defined software-engineering tasks that are integrated with management processes, and it must be performing them consistently. These requirements correspond directly with the ISO 9000-3 guidance for interpreting this clause.

As a practice in the Verifying Implementation common feature, the CMM identifies auditing to assure compliance with the specified standards and procedures.

One arguable correspondence is to the software process assets, including standards, procedures, and process descriptions, defined across the organization at level 3. Establishing such organizational assets would certainly contribute to implementing the quality system, but the standards and procedures in this clause could be addressed at the project level. ISO 9001 discusses the supplier's quality system, but it does not specifically address the relationship between organizational support and project implementation, as the CMM does.

ISO 9000-3, on the other hand, has two sections on quality planning: clause 4.2.3 discusses quality planning across projects; clause 5.5 discusses quality planning within a particular development.

### **G.1.1.3 Clause 4.3: Contract Review**

ISO 9001 requires organizations to review contracts to determine if requirements are adequately defined, agree with the bid, and can be implemented. The CMM addresses establishing a contract at level 2. The organization must document and review customer requirements, as allocated to software, and clarify any missing or ambiguous requirements. However, because the CMM is con-strained to the software perspective, customer requirements in general are beyond the scope of the Requirements Management key process area.

Also at level 2, the CMM describes the proposal, statement of work, and software-development plan that establish external (contractual) commitments, which the software-engineering group and senior management review.

Finally, the CMM explicitly addresses how the organization can acquire software through subcontracting with an external customer or other type of subcontractor (the supplier may also be a customer). ISO 9001's contract-review clause does not explicitly describe the supplier's role when it is acting as a customer to a subcontractor.

### CMM AND ISO 9000 DOCUMENT OVERVIEW

Below are highlights of the Capability Maturity Model Version 1.1 and ISO 9001 and 9000-3, the ISO 9000 standards that apply to software development and maintenance. For more detail on the CMM, see the CMM document.<sup>1,2</sup> For more details on using ISO 9000-3 and 9001, see those documents<sup>3,4</sup> and TickIt, the British guide for applying ISO 9001 to software.<sup>5</sup>

**CMM.** The Capability Maturity Model describes the principles and practices underlying software-process maturity and is intended to help organizations improve the maturity of their software processes through an evolutionary path from ad hoc, chaotic to mature, disciplined. It may also be used by an organization's customers to identify the strengths, weaknesses, and risks associated with their software suppliers. Authorized appraisers must go through both CMM and appraisal training. (For more information on CMM-based appraisal programs, contact SEI customer relations at (412) 268-5800.)

As Table A shows, the CMM is organized into five

levels. Except for level 1, each level has a set of key process areas that an organization should focus on to improve its software process. Each key process area comprises a set of key practices that indicate if the implementation and institutionalization of that area is effective, repeatable, and lasting.

For convenience, the key practices in each key process area are organized by common features:

- ◆ *Commitment to Perform.* What actions must the organization take to ensure that the process is established and will endure? Includes practices concerning policy and leadership.

- ◆ *Ability to Perform.* What preconditions must exist in the project or organization to implement the software process competently? Includes practices that concern resources, training, orientation, organizational structure, and tools.

- ◆ *Activities Performed.* What roles and procedures are necessary to implement a key process area? Includes practices on plans, procedures, work performed, tracking, and corrective action.

- ◆ *Measurement and Analysis.* What procedures

are needed to measure the process and analyze the measurements? Includes practices on process measurement and analysis.

- ◆ *Verifying Implementation.* What steps are needed to ensure that activities are performed in compliance with the established process? Includes practices on management reviews and audits.

Satisfying a key process area depends on both implementing and institutionalizing the process. Implementation is described in the Activities Performed common feature; institutionalization is described by the other common features.

**ISO 9001, 9000-3.** The ISO 9000 standards specify quality-system requirements for use when a contract between two parties requires the demonstration of a supplier's capability to design and supply a product. The two parties could be an external client and a supplier, or both could be internal, such as the marketing and engineering groups within the same company.

Of the ISO 9000 series, ISO 9001 is the standard most pertinent to software development and maintenance.

Organizations use it when they must ensure that the supplier conforms to specified requirements during several stages of development, including design, development, production, installation, and servicing. ISO 9000-3 provides guidelines for applying ISO 9001 to the development, supply, and maintenance of software.

Organizations typically use ISO 9000 standards to regulate their internal quality system and assure the quality system of their suppliers. In fact, the standards are frequently used to register a third-party's quality system. Certificates of registration have a defined scope within an organization and are issued by quality-system registrars. Auditors are trained in the ISO 9000 standards, but they may not be trained in or knowledgeable about software-specific issues. If the scope of an audit specifies software, software-knowledgeable auditors should be included on the auditing team.

**Status.** Version 1.1 of the CMM was published in February 1993. The SEI is now collecting change requests and investigating

TABLE A KEY PROCESS AREAS IN THE CMM	
Level	Key Process Areas
5 Optimizing Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.	Defect prevention Technology change management Process change management
4 Managed Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.	Quantitative process management Software quality management
3 Defined The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.	Organization process focus Organization process definition Training program Integrated software management Software product engineering Intergroup coordination Peer reviews
2 Repeatable Basic project-management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.	Requirements management Software project planning Software project tracking and oversight Software subcontract management Software quality assurance Software configuration management
1 Initial The software process is characterized as ad hoc, occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.	—

potential additions. The next release, planned for late 1996, may add key process areas and will harmonize the CMM with ISO 9001 and other standards. The ISO 9000 series was published in 1987. A minor revision to ISO 9001 was published in July 1994, and a major revision of the entire series is planned for 1996.

**REFERENCES**

1. M. Paulk et al., <i>Capability Maturity Model for Software, Version 1.1</i> , Tech. Report CMU/SEL-91-TR-24, Software Eng. Inst., Pittsburgh, 1993.	2. M. Paulk et al., <i>Key Processes of the Capability Maturity Model, Version 1.1</i> , Tech. Report CMU/SEL-93-TR-25, Software Eng. Inst., Pittsburgh, 1993.	3. <i>ISO 9000-1: Guidelines for the Application of ISO 9001 to the Development, Supply, and Maintenance of Software</i> , Int'l Org. for Standardization, Geneva, 1991.	4. <i>ISO 9001: Quality Systems — Model for Quality Assurance in Design/Development, Production, Installation, and Servicing</i> , Int'l Org. for Standardization, Geneva, 1994.	5. <i>TechIT: A Guide to Software Quality Management System Construction and Certification Using EN29001, Issue 2.0</i> , UK Dept. of Trade and Industry and the British Computer Society, London, 1992.
--	--	--	--	--

Table A. Key Process Areas in the CMM

### G.1.1.4 Clause 4.4: Design Control

ISO 9001 requires an organization to establish procedures to control and verify design. These include:

- planning, design, and development activities;
- defining organizational and technical interfaces;
- identifying inputs and outputs;
- reviewing, verifying, and validating the design; and
- controlling design changes.

ISO 9000-3 elaborates this clause with clauses on the purchaser’s requirements specification (5.3), development planning (5.4), quality planning (5.5), design and implementation (5.6), testing and validation (5.7), and configuration management (6.1).

The CMM describes the life-cycle activities of requirements analysis, design, code, and test at level 3. Level 2 addresses planning and tracking of all project activities, including these, as well as configuration management of software work products.

TABLE 1 SUMMARY MAPPING BETWEEN ISO 9001 AND THE CMM		
ISO 9001 Clause	Strong Relationship	Judgmental Relationship
4.1: Management responsibility	Commitment to perform Software project planning Software project tracking and oversight Software quality assurance	Ability to perform Verifying implementation Software quality management
4.2: Quality system	Verifying implementation Software project planning Software quality assurance Software product engineering	Organization process definition
4.3: Contract review	Requirements management Software project planning	Software subcontract management
4.4: Design control	Software project planning Software project tracking and oversight Software configuration management Software product engineering	Software quality management
4.5: Document and data control	Software configuration management Software product engineering	
4.6: Purchasing	Software subcontract management	
4.7: Control of customer-supplied product	—	Software subcontract management
4.8: Product identification and traceability	Software configuration management Software product engineering	
4.9: Process control	Software project planning Software quality assurance Software product engineering	Quantitative process management Technology change management
4.10: Inspection and testing	Software product engineering Peer reviews	
4.11: Control of inspection, measuring, and test equipment	Software product engineering	
4.12: Inspection and test status	Software configuration management Software product engineering	
4.13: Control of nonconforming product	Software configuration management Software product engineering	
4.14: Corrective and preventive action	Software quality assurance Software configuration management	Defect prevention
4.15: Handling, storage, packaging, preservation, and delivery	—	Software configuration management Software product engineering
4.16: Control of quality records	Software configuration management Software product engineering Peer reviews	
4.17: Internal quality audits	Verifying implementation Software quality assurance	
4.18: Training	Ability to perform Training program	
4.19: Servicing	—	
4.20: Statistical techniques	Measurement and analysis	Organization process definition Quantitative process management Software quality management

Table 1. Summary Mapping Between ISO 9001 and the CMM

ISO 9001, as revised in 1994, requires design reviews. ISO 9000-3 states that the supplier should carry out reviews to ensure that requirements are met and design methods are correctly carried out. However, although design reviews are required, organizations have a range of options for satisfying this clause, from technical reviews to inspections. In contrast, the CMM specifically calls out peer reviews at level 3 and identifies a number of work products that should undergo such a review.

TickIt training clarifies the ISO 9001 perspective by listing three examples of design reviews: Fagan inspections, structured walkthroughs, and peer reviews (in the sense of a desk check). The training also states (on page 17.10) that “an auditor will need to be satisfied from the procedures and records available that the reviews with-in an organization are satisfactory considering the type and criticality of the project under review.”<sup>1</sup>

The CMM describes more formal, quantitative aspects of the design process at level 4, but ISO 9001 does not require this degree of formality.

### **G.1.1.5 Clause 4.5: Document and Data Control**

ISO 9001 requires an organization to control the distribution and modification of documents and data. The CMM describes the configuration-management practices characterizing document and data control at level 2. The documentation required to operate and maintain the system is specifically called out at level 3. The specific procedures, standards, and other documents that may be placed under configuration management are identified in the different key process areas in the Activities Performed common feature.

### **G.1.1.6 Clause 4.6: Purchasing**

ISO 9001 requires organizations to ensure that purchased products conform with specified requirements. This includes evaluating potential subcontractors and verifying purchased products.

The CMM addresses custom soft-ware development at level 2, including the evaluation of subcontractors and acceptance testing of subcontracted software.

### **G.1.1.7 Clause 4.7: Control of Customer-Supplied Product**

ISO 9001 requires an organization to verify, control, and maintain any customer-supplied material. ISO 9000-3 discusses this clause in the con-text of included software product (6.8), also addressing commercial-off-the-shelf software.

The only CMM practice describing the use of purchased software is a sub-practice at level 3, and the context is identifying off-the-shelf or reusable software as part of planning. The integration of off-the-shelf and reusable software is one of the CMM’s weaker areas. In fact, this clause, especially as expanded in ISO 9000-3, cannot be considered adequately covered by the CMM. It would be reasonable, though not sufficient, to apply the acceptance testing practice for subcontracted soft-ware at level 2 to any included soft-ware product.

I have written a change request to CMM version 1.1 to incorporate practices that address product evaluation and the inclusion of off-the-shelf soft-ware and other types of software that have not been developed internally.

### **G.1.1.8 Clause 4.8: Product Identification and Traceability**

ISO 9001 requires an organization to be able to identify and trace a product through all stages of production, delivery, and installation. The CMM covers this clause primarily at level 2 in the context of configuration management, but states the need for consistency and traceability between software work products at level 3.

### **G.1.1.9 Clause 4.9: Process Control**

ISO 9001 requires an organization to define and plan its production processes. This includes carrying out production under controlled conditions, according to documented instructions. When an organization cannot fully verify the results of a process after the fact, it must continuously monitor and control the process. ISO 9000-3 clauses include design and implementation (5.6); rules, practices, and conventions (6.5); and tools and techniques (6.6).

In the CMM, the specific procedures and standards that would be used in the software-production process are specified in the software-development plan at level 2. The definition and integration of software-production processes, and the tools to support these processes, are described at level 3. Level 4 addresses the quantitative aspect of control, exemplified by statistical process control, but an organization typically would not have to demonstrate this level of control to satisfy this clause. Also, clause 6.6 in ISO 9000-3 states that “the supplier should improve these tools and techniques as required.” This corresponds to transitioning new technology into the organization, a level 5 focus.

### **G.1.1.10 Clause 4.10: Inspection and Testing**

ISO 9001 requires an organization to inspect or verify incoming materials before use and to perform in-process inspection and testing. The organization must also perform final inspection and testing before the finished product is released and keep inspection and test records. I have already described how the CMM deals with issues surrounding the inspection of incoming material (“Clause 4.7: Control of customer-supplied product”). The CMM describes testing and in-process inspections (strictly for software) at level 3.

### **G.1.1.11 Clause 4.11: Control of Inspection, Measuring, and Test Equipment**

ISO 9001 requires an organization to control, calibrate, and maintain any equipment used to demonstrate conformance. When test hardware or software is used, it must be checked before use and rechecked at prescribed intervals. ISO 9000-3 clarifies this clause with clauses on testing and validation (5.7); rules, practices, and conventions (6.5); and tools and techniques (6.6).

The CMM generically addresses this clause under the testing practices in Software Product Engineering. Test software is specifically called out in the Ability to Perform common feature in the practice that describes tools that support testing (Ability 1.2).

### **G.1.1.12 Clause 4.12: Inspection and Test Status**

ISO 9001 requires an organization to maintain the status of inspections and tests for items as they move through various processing steps. The CMM addresses this clause with practices on problem reporting and configuration status at level 2 and by testing practices at level 3.

### **G.1.1.13 Clause 4.13: Control of Nonconforming Product**

ISO 9001 requires an organization to control a nonconforming product — one that does not satisfy specified requirements — to prevent inadvertent use or installation. ISO 9000-3 maps this concept to clauses on design and implementation (5.6); testing and validation (5.7); replication, delivery, and installation (5.9); and configuration management (6.1).

The CMM does not specifically address nonconforming products. In ISO 9000-3, the control issue essentially disappears among a number of related processes spanning the soft-ware life-cycle. In the CMM, the status of configuration items, which would include the status of items that contain known defects not yet fixed, is maintained at level 2. Design, implementation, testing, and validation are addressed at level 3.

### **G.1.1.14 Clause 4.14: Corrective and Preventive Action**

ISO 9001 requires an organization to identify the causes of a nonconforming product. Corrective action is directed toward eliminating the causes of actual nonconformities. Preventive action is directed toward eliminating the causes of potential nonconformities. ISO 9000-3 quotes this clause verbatim, with no elaboration, from the 1987 release of ISO 9001.

A literal reading of this clause would imply many of the CMM's practices in the level 5 key process area, Defect Prevention. According to the TickIt auditors' guide 4 (pages 139- 140) and discussions with ISO 9000 auditors, corrective action is driven primarily by customer complaints. The software-engineering group should look at field defects, analyze why they occurred, and take corrective action. This would typically occur through software updates and patches distributed to the fielded software.

Under this interpretation of the clause, an appropriate mapping would be to level 2's problem reporting, followed by controlled maintenance of baselined work products.

Another interpretation described in section 23 of the TickIt training literature<sup>1</sup> is that corrective action is to address noncompliance identified in an audit, whether external or internal. This interpretation maps to the CMM's level 2 key process area, Software Quality Assurance. How you interpret "preventive action" is a controversial issue in applying ISO 9001 to software. Some auditors seem to expect a defect-prevention process similar to that found in a manufacturing environment. Others require only that an organization address user-problem reports. It is debatable how much of the CMM's level 5 in-process causal analysis and defect prevention is necessary to satisfy this clause.

### **G.1.1.15 Clause 4.15: Handling, Storage, Packaging, Preservation, and Delivery**

ISO 9001 requires organizations to establish and maintain procedures for handling, storage, packaging, and delivery. ISO 9000-3 maps this to clauses on acceptance (5.8) and replication, delivery, and installation (5.9).

The CMM does not cover replication, delivery, and installation. It addresses the creation and release of software products at level 2, and acceptance testing at level 3. The CMM does not, however, describe practices for delivering and installing the product. I have written a change request to CMM version 1.1 to incorporate a practice for these areas.

### **G.1.1.16 Clause 4.16: Control of Quality Records**

ISO 9001 requires an organization to collect and maintain quality records. In the CMM, the practices defining the maintenance of quality records are distributed throughout the key process areas as part of the Activities Per-formed common feature. Specific to this clause are the problem reporting described at level 2 and the testing and peer review practices, especially the collection and analysis of defect data, at level 3.

### **G.1.1.17 Clause 4.17: Internal Quality Audits**

ISO 9001 requires an organization to plan and perform audits. The results of audits are communicated to management, and any deficiencies found are corrected.

The CMM describes the auditing process at level 2. Auditing practices to ensure compliance with the specified standards and procedures are identified in the Verifying Implementation common feature.

### **G.1.1.18 Clause 4.18: Training**

ISO 9001 requires an organization to identify training needs, provide training (since selected tasks may require qualified personnel), and maintain training records.

The CMM identifies specific training needs in the training and orientation practices in the Ability to Perform common feature. It describes the general training infrastructure, including maintaining training records, at level 3.

### **G.1.1.19 Clause 4.19: Servicing**

ISO 9001 requires an organization to perform servicing activities when such activities are part of a specified requirement. ISO 9000-3 addresses this clause as maintenance (5.10). Although the CMM is intended to be applied in both the software development and maintenance environments, the practices in the CMM do not directly address the unique aspects that characterize the maintenance environment. Maintenance is embedded throughout the CMM, but organizations must correctly interpret these practices in the development or maintenance context. Maintenance is not, therefore, a separate process in the CMM. Change requests for CMM version 1.0 expressed a concern about using the CMM for maintenance projects, and the SEI changed some wording for CMM version 1.1 to better address the maintenance environment. The SEI anticipates that this will remain a topic of discussion as it pro-vides guidance for tailoring the CMM to different environments, such as maintenance, and begins the next revision cycle for the CMM.

### **G.1.1.20 Clause 4.20: Statistical Techniques**

ISO 9001 states that organizations must identify adequate statistical techniques and use them to verify the acceptability of process capability and product characteristics. ISO 9000-3 simply characterizes this clause as measurement (6.4).

In the CMM, product measurement is typically incorporated into the various practices within the Activities Performed common feature. Process measurement is described as part of the Measurement and Analysis common feature.

Level 3 describes the establishment of an organization-wide process data-base for collecting process and product data. It seems likely that most auditors would accept project-level data (as described at level 2) to satisfy this clause. However, at least a few auditors require an organization-level historical database and the use of simple statistical control charts.

If you infer statistical process control from this clause, an organization would satisfy it at level 4. To quote ISO 9000-3, however, “there are currently no universally accepted measures of software quality.” Some auditors look for the use of statistical tools, such as Pareto analysis. Others are satisfied by any consistently collected and used measurement data. In general, the only absolute is that auditors vary significantly in how they interpret this clause.

---

## G.1.2 Summary

Clearly there is a strong correlation between ISO 9001 and the CMM, although some issues in ISO 9001 are not covered in the CMM, and vice versa. The level of detail differs significantly: section 4 in ISO 9001 is about five pages long; sections 5, 6, and 7 in ISO 9000-3 comprise about 11 pages; and the CMM is more than 500 pages. Judgment is needed to determine the exact correspondence, given the different levels of abstraction.

As Table 1 shows, the clauses in ISO 9001 with no strong relationships to the CMM key process areas, and that are not well addressed in the CMM, are control of customer-supplied product (4.7) and handling, storage, packaging, preservation, and delivery (4.15). The clause in ISO 9001 that is addressed in the CMM in a completely distributed fashion is servicing (4.19). The clauses in ISO 9001 for which the exact relationship to the CMM is subject to significant debate are corrective and preventive action (4.14) and statistical techniques (4.20).

As I stated earlier, the biggest difference between the two documents is the explicit emphasis of the CMM on continuous process improvement. ISO 9001 addresses only the minimum criteria for an acceptable quality system. Another difference is that the CMM focuses strictly on software, while ISO 9001 has a much broader scope that encompasses hardware, software, processed materials, and services.

The biggest similarity between the two documents is their bottom line: “Say what you do; do what you say.” The fundamental premise of ISO 9001 is that organizations should document every important process and check the quality of every deliverable through a quality-control activity. ISO 9001 requires documentation that contains instructions or guidance on what should be done or how it should be done. The CMM shares this emphasis on processes that are documented and practiced as documented. Phrases such as conducted “according to a documented procedure” and following “a written organizational policy” characterize the key process areas in the CMM.

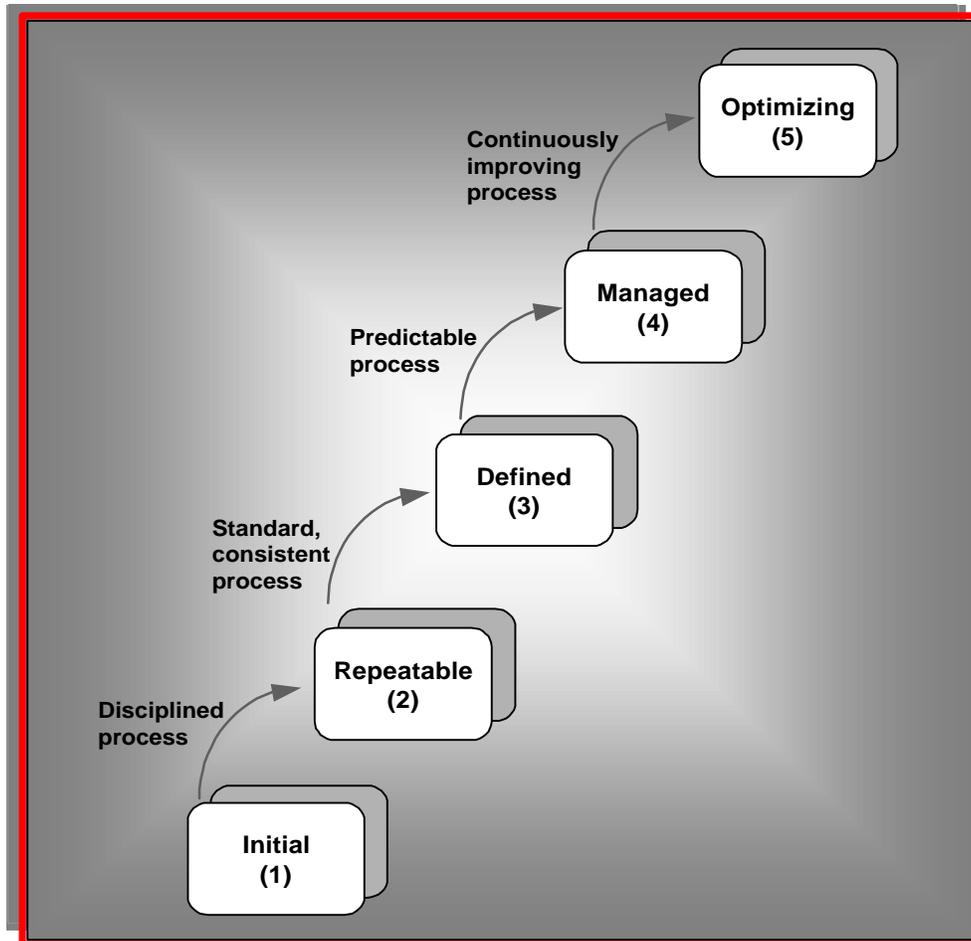


Figure 1. Key Process Area Profile for an ISO 9001-Compliant Organization.

Figure 1: Dark shading represents practices that ISO 9001 or ISO 9000-3 directly address; light shading indicates practices that may be addressed, depending on how you interpret ISO 9001; and unshaded areas indicate practices not specifically addressed.

On a more detailed level, some clauses in ISO 9001 are easily mapped to their equivalent CMM practices. Other relationships map in a many-to-many fashion, since the two documents are structured differently. For example, the training clause (4.18) in ISO 9001 maps to both the Training Program key process area and the training and orientation practices in all the key process areas.

### G.1.3 Compliance Issues

At first glance, an organization with an ISO 9001 certificate would have to be at level 3 or 4 in the CMM. In reality, some level 1 organizations have been certified. One reason for this discrepancy is ISO 9001's high level of abstraction, which causes auditors to interpret it in different ways. If the auditor certifying the organization has had TickIt training, for example, the design reviews in ISO 9001 will correspond directly to the CMM's peer reviews, which are at level 3. But not all auditors are well-versed in software development. The virtue of a program like TickIt is that it produces auditors who understand how to apply ISO 9001 to software.

Another reason for the discrepancy is that an auditor may not require mastery to satisfy the corresponding ISO 9001 clause.

Figure 1 shows how an ISO-9001 compliant organization that has implemented no other management or engineering practices except those called out by ISO 9001 rates on the CMM. The size of the bar indicates the percentage of practices within the key process area that are addressed in either ISO 9001 or ISO 9000-3. The figure shows areas that have a direct relationship to clauses in these documents (dark shading), areas for which the relationship is subject to interpretation (light shading), and areas that the clauses do not directly address (white). Note the following about Figure 1:

- Every key process area at level 2 is strongly related to ISO 9001.
- Every key process area is at least weakly related to ISO 9001 under some interpretation.

On the basis of this profile, an organization assessed at level 1 could be certified as compliant with ISO 9001. That organization would, however, have to have significant process strengths at level 2 and noticeable strengths at level 3. Private discussions indicate that many level 1 organizations have received ISO 9001 certificates. If an organization is following the spirit of ISO 9001, it is likely to be near or above level 2. However, organizations have identified significant problems during a CMM-based assessment that had not surfaced during a previous ISO 9001 audit.<sup>5</sup> This seems to be related to the greater depth of a CMM-based investigation.

Although the CMM does not adequately address some specific issues, in general it encompasses the concerns of ISO 9001. The converse is less true. ISO 9001 describes only the minimum criteria for an adequate quality-management system, rather than addressing the entire continuum of process improvement, although future revisions of ISO 9001 may address this concern. The differences are sufficient to make a rigid mapping impractical, but the similarities provide a high degree of overlap.

To answer the three questions I listed in the beginning of this article:

- An ISO 9001-compliant organization would not necessarily satisfy all the key process areas in level 2 of the CMM, but it would satisfy most of the level 2 and many of the level 3 goals. Further, because ISO 9001 doesn't address all the CMM practices, a level 1 organization could receive ISO 9001 registration.
- A level 2 (or 3) organization would probably be considered compliant with ISO 9001 but even a level 3 organization would need to ensure that it adequately addressed the delivery and installation process described in clause 4.15 of ISO 9001, and it should consider the use of included software products, as described in clause 6.8 of ISO 9000-3. With this caveat, obtaining certification should be relatively straightforward for a level 2 or higher organization.
- As to whether software process improvement should be based on the CMM or ISO 9001, the short answer is that an organization may want to consider both, given the significant degree of overlap. A market may require ISO 9001 certification; addressing the concerns of the CMM would help organizations prepare for an ISO 9001 audit. Conversely, level 1 organizations would certainly profit from addressing the concerns of ISO 9001. Although either document can be used alone to structure a process-improvement program, the more detailed guidance and software specificity provided by the CMM suggests that it is the better choice, although admittedly this answer may be biased.

In any case, organizations should focus on improvement to build a competitive advantage, not on achieving a score — whether that is a maturity level or a certificate. The SEI advocates addressing continuous process improvement as encompassed by the CMM, but even then there is a need to address the larger business context in the spirit of Total Quality Management.

---

## G.2 Acknowledgements

I thank the many people who commented on the early drafts of this article and who discussed the relationships between ISO 9001 and the CMM. In some cases, we have agreed to disagree, but the discussions were always interesting. Specifically, I thank Peter Anderson, Robert Bamford, Kelley Butler, Gary Coleman, Taz Daughtrey, Darryl Davis, Bill Deibler, Alec Dorling, George Kambic, Dwight Lewis, Stan Magee, Helen Mooty, Don O'Neill, Neil Potter, Jim Roberts, John Slater, and Charlie Weber. This work is sponsored by the US Department of Defense under contract F19628-90-C-003.

---

## G.3 References

1. Lloyd's Register TickIT Auditors' Course, Issue 1.4, Lloyd's Register, Mar. 1994.
2. Mark C. Paulk, "A Comparison of ISO 9001 and the Capability Maturity Model for Software," Tech. Report CMU/SEI-94-TR-2, Software Eng. Inst., Pittsburgh, July 1994.
3. M. Paulk, "Comparing ISO 9001 and the Capability Maturity Model for Software," Software Quality J., Dec. 1993, pp. 245-256.
4. TickIT: A Guide to Software Quality Management System Construction and Certification Using EN29001, Issue 2.0, UK Dept. of Trade and Industry and the British Computer Society, London, 1992.
5. F. Coallier, "How ISO 9001 Fits Into the Software World," IEEE Software, Jan. 1994, pp. 98-100.

---

## G.4 Biography

Mark C. Paulk is a senior member of the technical staff at the Software Engineering Institute, where he is product manager for version 2 of the Capability Maturity Model. At the SEI, he was also project leader for the CMM version 1.1 development. Before joining the SEI, Paulk worked on distributed real-time systems for System Development Corp. (later Unisys Defense Systems) at the Ballistic Missile Defense Advanced Research Center. Paulk received a BS in mathematics from the University of Alabama, Huntsville, and an MS in computer science from Vanderbilt University. He is a senior member of the IEEE and a member of the American Society for Quality Control.

Address questions about this article to Paulk at Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890; mcp@sei.cmu.edu.