A COMPARISON OF ISO 9000 AND SEI/CMM FOR SOFTWARE ENGINEERING ORGANIZATIONS

Hiranmay Ghosh[*]

Abstract: ISO 9000 and CMM are two well-established models for Software Quality System. This paper compares the two models in detail and analyses how they can be used to complement each other in establishing a Quality System by a Software Engineering Organization.

1. INTRODUCTION

A Process Improvement program or a Capability Evaluation of the potential contractors requires benchmarking of the Quality System in an organization following a well-defined, commonly understood and universally accepted model. Besides ISO 9000, which is almost universally accepted for all segments of the industry, there are quite a few other models proposed specifically for benchmarking Software Engineering organizations. The Capability Maturity Model (CMM) formulated by the Software Engineering Institute (SEI) is one of the most popular among such models. While ISO 9000 sets some standards to qualify for a certification, the CMM attempts to grade a Software Development Organization on a five-level Process Maturity scale.

While both the models are aimed at providing a capability of delivering Quality with *consistency* and at providing a framework for *Quality Improvement* of the Software product or services, there are some differences in their approaches. The existence of two models, each of which is aimed as a frame of reference for Quality Systems, has triggered many a thought to compare the two models and to set some equivalence between them[6,7,8]. In this respect, some commonly asked questions are — if an organization is ISO 9000 certified, to which level of the CMM does it qualify for? Conversely, if an organization is rated at a certain level of the CMM, does it qualify for an ISO 9000 certification? Is such a comparison really possible?

While most of such discussions center around the Capability Evaluation and Certification issues, the focus of this article is on the use of the models for (I) establishing a Quality System and (ii) undertaking a Process Improvement program. The commonalties and the differences of the two models have been brought out by analyzing their requirements in details. The intention here is not to find an equation between the two models, but to explain how the two models do complement each other and can be used together by a software engineering organization to establish an effective Quality System.

2. THE ISO 9000 AND SEI/CMM

This section introduces ISO 9000 and SEI/CMM for a preliminary acquaintance. For a detailed understanding, the documents 1-5 may be referred to.

2.1. ISO 9000 Model

The ISO 9000 series of standards for Quality System is the result of the efforts of an international technical working group, working under the aegis of the ISO. The work is a build-up primarily on earlier American and British Quality Systems Standards, MIL-Q-9858 and BS5750. Though the ISO 9000 series of standards are applicable to any type of industry, there is a notable terminological bias towards the manufacturing sector. This is probably because quality problems were first experienced with the mass-produced commodities in post-World War II era.

ISO 9000 comes as a set of documents in multiple parts. Three documents in the series are important for a Software Engineering organization. ISO 9001[1] (published: 1987, revised: 1994) is the applicable standard, to which a software engineering organization must comply in order to qualify for a certification. It specifies the requirements of a Quality System in twenty major clauses that cover all aspects of business; typical examples are management responsibilities, engineering processes such as design, process control and testing, and support processes such as purchase, materials handling and training. ISO 9000-3[2] (published: 1991) provides the guidelines for interpreting ISO 9001 for software development and elaborates primarily on issues specific to Software Engineering such as Requirements Management,

* Centre for Development of Telematics, 9th floor, Akbar Bhawan, New Delhi 110021, INDIA. Internet: ghosh@cdotd.ernet.in

0-7803-2608-3

Configuration Management and Metrics. ISO 9004-1[3] (published: 1987, revised: 1994) is a guideline to Quality System elements in an organization.

We shall primarily refer to these documents for discussions on the ISO model. A general reference to "ISO 9000" in the following text will mean reference to either of these three documents or to any other supporting document in the series.

2.2. The Capability Maturity Model

The Capability Maturity Model (CMM) has been developed by the Software Engineering Institute (SEI) of the Carnegie-Mellon University (CMU) as a project sponsored by the Department of Defense (DoD), USA. The primary objective of the project was to establish a method for evaluating the capability of the DoD contractors in delivering quality software. The CMM attempts to classify the software development organizations at five levels of process-maturity. Level-1 is the "initial" level, where software development takes place without any systematic approach and the success depends on individual effort. At level-2, called "repeatable", the basic management processes are established and the successful practices of the earlier projects are repeated. At level-3, the engineering and management processes are "defined" and institutionalized. At level-4, the "managed" level, the process and the product qualities are quantitatively measured, understood and controlled. Finally, at the highest "optimizing" level, level-5, the organization learns to analyze the quantitative feedback from the processes and to improve upon them continuously through innovative ideas and technologies.

The CMM suggests that the process maturity of an organization has to develop necessarily from level-1 to level-5 progressively through the intermediate levels, without any possibility of a short-cut. It defines certain key process areas, which need to be addressed at each level. A key process area of a lower level is necessarily a prerequisite to that of a higher level, for example, a process definition (level-3) being a prerequisite to a process measurement (level-4) and improvement (level-5). In summary, it recommends that, the management processes, rather than the technical ones, should be established in an organization first. The reason is that, when there is an emergency in an organization, engineering processes are likely to get washed away unless adequately supported by the management.

The CMM has been formalized in the form of two technical reports "The Capability Maturity Model"[4] and "The Key Practices of the CMM"[5] (both published: 1989, revised: 1993). The first document builds up the basic framework of the model and defines the key process areas that need to be progressively addressed to reach the various capability levels. The second document describes the key practices of each of the process areas in terms of goals, commitments, abilities and activities; it can be used as a guideline to implement the processes and thereby graduate from one maturity level to the next.

3. BROAD COMPARISON OF ISO 9000 AND CMM

As a prelude to a detailed comparison, a broad comparison of the two models are presented in this section. It may be worthwhile to understand the major commonalties and differences of the two models before having a more detailed look.

3.1. Major Commonalties

Though there is a difference in approach, both the ISO 9000 and the CMM tend to capture the same essentials of a Quality System. The major commonalties between the two models can be summarized as follows:

1. Both ISO 9000 and CMM aim at capability to deliver Quality with *consistency*.
2. Both aim at *Quality Improvement* of the products or services.
3. Both stress that quality assurance should be a *planned activity,* i.e. quality may not be achieved by accident.
4. Both require *management commitment* to quality expressed through appropriate explicit *policy* statement(s).
5. Both require that the errors should be *prevented* rather than corrected.
6. Both require that there should be defined and documented *processes* in the organization.
7. Both require that the processes should be *followed* and *monitored.*
8. Both require that the results of the activities are *recorded.*
9. Both require that the effectiveness of the processes be *reviewed* by *an appropriate level of management.*
10. Both require that the processes are *continuously improved* upon.

3.2. Major Differences

The major differences between the ISO 900 and the CMM can be summarized as follows:

1. ISO 9000 applies to any type of industry; CMM is developed specifically for software industry.
2. ISO 9000 addresses corporate business processes as a whole; CMM primarily focuses on software engineering activities.
3. While ISO 9000 specifies some minimum requirements, CMM gets into more details of the technical aspects of software engineering.
4. While ISO 9000 restricts itself to *what* is required, CMM suggests *how to* fulfill the requirements also.
5. While ISO 9000 provides a pass/fail criterion, CMM provides for a gradation for process maturity.
6. While ISO 9000 does not specify the sequence of steps required to establish a Quality System, CMM recommends a mechanism for step-by-step progress through its successive maturity levels.
7. Certain process elements are discussed in ISO 9000 but not explicitly in CMM; similarly, some other process elements are discussed only in CMM and not explicitly in ISO 9000 (See Table-1). However, there are indirect reference to each of these process elements in both the models.

documents[1-3], and the CMM documents, namely the "Capability Maturity Model" and the "Key Practices of the CMM" [4-5]

In the following text, we first compare the scope and the purview of the two models, and then the recommendations in the two models for the various processes applicable to a software engineering organization. For the purpose of comparison, the processes are partitioned into three major categories, namely the *Management/Support Processes*, the *Organizational Processes* and the *Engineering Processes*. The management/support processes refer to the typical project management and support activities such as requirements management and configuration management. The organizational processes refer to cross-project management functions such as training. The engineering processes refer to the product engineering such as design, testing and reviews. It may be noted that the processes are not totally independent of each other, and therefore there is some duplication of text while comparing them.

There are two general commonalties of the models, which are applicable to all the processes. The first is that there should be a documented procedure, including responsibility definition, for every job-function. The second one is that records of all the activities are to be maintained. These requirements make both the models primarily document-driven, a fact that is hated by many professionals.

The points presented below, collectively, do not represent the complete recommendations of either ISO 9000 standards or the CMM. The notable requirements of the two models are presented in the following text for the purpose of comparison.

Table 1: Process Elements unique to ISO 9000 and SEI/CMM

Process Elements unique to ISO 9000	Process Elements unique to CMM
1. Contract Management (beyond requirements)	1. Project Tracking and Oversight
2. Purchase and Customer Supplied components	2. Process and Technology Change Management
3. Personnel issues (beyond training)	3. Intergroup coordination to meet customer requirements.
4. Package, Delivery and Installation	4. Organization-wide Process Focus, Process Development and Integrated Management.

4. DETAILED COMPARISON OF ISO 9000 AND CMM

A detailed comparison of the two quality system frameworks is presented in this section. The comparison is based on the information presented in the ISO 9000 documents relevant for software engineering, namely ISO 9001, 9000-3 and 9004-1

4.1. Scope and Purview

The scope of ISO 9001 is "for demonstration of supplier's capability" in case of a contractual situation. ISO 9000-3 interprets ISO 9001 for software engineering organizations. ISO 9004-1 describes the basic set of quality system elements. Thus, the three

documents collectively establish a basic framework for quality system and provide standards for capability determination of a software engineering organization. CMM, on the other hand, provides a maturity framework for software engineering processes. Besides capability determination, it is aimed to be used for process (self) assessment and process improvement.

While the latter purposes are not explicitly mentioned in ISO 9000 documents, internal audits provide for a means of self-assessment and process improvement is implicit in the form of endeavors to meet the requirements of the standard and in the form of corrective and preventive actions.

4.2. Management/Support Processes:

The CMM recommends participation by the engineering staff in the management functions such as requirements management and project management. In particular, CMM makes it absolutely important that the management decisions be reviewed and agreed upon by the engineering staff and that the latter commits to the decisions during the execution of the project. These are some operational requirements for the success of the quality system, which are not explicit in the ISO 9000 documents.

Some of the management/support processes are compared in greater details below. CMM classifies all of these management/support processes as key process areas of maturity level-2.

4.2.1. Contract and Requirements Management

Both the models call for a review of the requirements by all appropriate functions, the definition of the requirements to form a baseline for project planning, and that any changes therein to be appropriately controlled. While ISO 9000 discusses contract (including requirements) management in general, CMM focuses specifically on requirement management. Additionally, both the models require that the customer requirements or the terms of the contract and the commitments required in fulfilling them be reviewed, understood and be agreed upon by all relevant personnel and groups.

4.2.2. Project Planning and Monitoring

Both the models call for a documented project-plan with defined responsibilities and its use in project tracking. Definition of phases (life-cycle) is one important aspect of planning in both the models. However, there are some differences in the importance assigned to the other aspects of the planning process. ISO 9000 stresses on adequate resources, qualified personnel, clarity of objectives and identification of plans for the support activities, such as quality assurance, configuration management, integration and test. CMM stresses on use of formal estimates in planning, review of external commitments and control of the changes in the plan.

It may be noted that all the aspects described either in ISO 9000 or in CMM are equally important for software project management. While some of the points are explicitly mentioned in either of these documents, the others follow by deduction.

4.2.3. Quality Assurance

Both the models call for a planned quality assurance activity in an organization. While none of the models require a dedicated group for quality assurance, both call for clear assignment of quality responsibilities. ISO 9000 requires a clear definition of quality objectives and stresses on avoiding non-compliance at every stage of development to meet the quality objectives. It stresses on reviews, tests and other V&V activities at the various stages of development to avoid non-compliance's to proliferate further down the life-cycle. CMM, on the other hand, stresses on the involvement of all relevant personnel, including senior management, in implementing the quality system, an explicit quality assurance plan and the participation of the quality assurance group in project planning. Both the models call for periodic and need based review of quality system (audits) and management review of the effectiveness of quality system.

4.2.4. Configuration Management

ISO 9000 refers to Configuration Management through requirements and design change control, documentation control, product identification and traceability. Both the models calls for identification, change control and availability of configuration items. CMM explicitly recommends the establishment of a CM library for software baseline and configuration audits.

4.2.5. Subcontract and Purchase Management

Both the models stress on assuring quality of imported components, which will affect the overall quality of the product or services being offered by the supplier. ISO 9000 explicitly classifies such components as purchased components, subcontracted components and customer-supplied components. It makes the supplier responsible for ensuring the quality of all the three types of imported components. CMM has explicit reference to subcontracted components alone, probably because, it is more prevalent in software industry than

the other two types. Both the models require an objective pre-qualification of vendors based on the evaluation of their quality system. ISO 9000 relies on unambiguous purchase specification and inspection of in-coming components to ensure quality of an imported component; CMM relies more on the review of subcontractors' quality systems and tracking of their activities.

4.3. Organizational Processes

4.3.1. Management of Quality System

Both the models hold the management of the supplier organization to be responsible for the quality of the products or services it offers. Responsibility definition and allocation of adequate resources (including qualified personnel and training) are the prime responsibilities of the management in implementing a quality system. The management's intention (the quality goals of an organization) is to be expressed through appropriate policy statement(s). ISO 9000 recommends quality objectives, costs and alignment to other organizational objectives to be the major considerations for the quality policy. CMM requires all individual processes in an organization to be governed by an appropriate policy statement. Both the models recommend periodic and need-based review of the quality system by an appropriate level of management. In CMM documents, these requirements are distributed over the key processes at various levels.

4.3.2. Process and Technology Management

Both the models require that every activity in an organization follow a documented procedure, which is a part of the Quality System. CMM requires that the processes followed in the various projects or departments of an organization to be synthesized into a "standard" software process definition for the organization. It also recommends appropriate tailoring of the standard process for the projects to suit their specific needs. Both the models recommend the use of appropriate technology as a part of the Quality System.

ISO 9000 recommends the cost and the effectiveness of the Quality System to be reviewed in economic perspective and the result of such review be the basis of process and technology improvement. CMM calls for continuous improvement of process and technology through assessment of needs, evaluation of new technology, analysis of benefits, pilot trials and global participation.

Both the models recommend the use of metrics (statistical techniques) for quantitative process-control and to establish process-capability baseline. Being sensitive to "customer satisfaction", ISO 9000 specifies the use of appropriate metrics to reflect product-fault related data from customer's viewpoint to be a minimum requirement. While the process development is addressed in level-3, quantitative process management and improvement are addressed in levels 4 and 5 respectively of the CMM.

4.3.3. Personnel and Training

Both the models call for necessary training for the personnel performing any job-function (engineering or management) within a quality system. CMM calls for a project-level and organization level training plans. While CMM restricts itself to training, ISO 9000 points out the importance of other personnel issues, such as educational qualifications, experience and motivation towards successful implementation of a quality system. Training is a key process area of level-3 of CMM.

4.4. Engineering Processes

4.4.1. Product Engineering

Each of the models explicitly states that it is quite general and does not assume any particular life-cycle model for software. However, both of them identify the basic engineering functions for software development and maintenance. In CMM, these functions are requirement engineering, design, code development and testing. ISO 9000 excludes requirements engineering from the list, probably considering it to be adequately covered as a part of contract review. In order to achieve quality, ISO 9000 stresses on control and verification of design, controlled process and environment and testing of incoming components, semi-finished products and the final product. CMM stresses on definition, integration and consistent performance of the engineering tasks and consistency of the work-products with one another. Additionally, ISO 9000 recommends identification of inputs, outputs, and verification method for every engineering function, which is similar to the ETVX paradigm[9], task-definition being implicit in a 'documented' quality system. There is no such recommendation in the CMM. Product Engineering is placed at level-3 of CMM.

4.4.2. Technical (Peer) Reviews

Both the models recommend review of work-products to prevent mistakes committed in one life-cycle phase from percolating down to the subsequent phases. ISO 9000 recommends development reviews at appropriate points in the development phases; there are no

comments on the nature of such reviews. CMM recommends these reviews to be conducted by peer groups and requires the reviews to be planned, conducted and recorded. Peer Review is a key process area of level-3 of CMM.

4.4.3. Defect Prevention

ISO 9000 requires appropriate corrective and preventive actions to be undertaken based on a review of product and process quality attributes. Contrasting with the section on disposition of defective products, it may be interpreted that these actions are really process improvements in reaction to actual and anticipated defects. CMM stresses on identification of common causes to the defects, and systematic elimination of such causes through prioritization, revision of procedures and standards and implementation of the revised documents. Defect Prevention is addressed at level-5 of CMM.

5. CONCLUSIONS

From the preceding discussions, it is evident that most of the requirements of ISO 9000 and CMM are quite similar. The requirements, where they differ, are complementary, rather than being supplementary. While ISO 9000 covers the overall business activities of an organization, CMM focuses more on the (software) engineering aspects. Thus, the two models can be used together to an organization's advantage for ensuring coverage as well as depth in the core engineering area.

Both the models are premised on the four basic Quality Management principles, namely, (i) prevention of defects, (ii) focus on process, (iii) use of quantitative goals and measurements and (iv) review and improvements. Either of the models can be followed to develop a Quality System in a software organization, and the results could be equally satisfactory. It may be noted that, the requirements of ISO 9000 are distributed over all the levels of CMM, (excluding level-1, which is *chaotic* anyway!) rather than being confined to the lower levels. Contrary to the common belief, if followed in spirit, the ISO 9000 model can be used to establish a Quality System with maturity equivalent to CMM level-5's.

ISO 9000 documents are, in comparison to CMM, very abstract in nature and are subject to wide interpretation differences. The minimum requirements of a ISO 9000 certified "Quality System" may vary, depending on the assessor or the assessment agency involved, and the results of an assessment may not be repeatable. Thus it is quite possible that an organization at a relatively low maturity level in the CMM scale, gets qualified for a ISO 9000 certification. CMM, being more elaborate sets far more objective criteria for attainment of a maturity level, though scope of subjectivity cannot be totally ruled out. The objectivity is further augmented by the standard support tools with the CMM, such as a standard set of Maturity Questionnaire.

While ISO 9000 specifies the requirements of a quality system, CMM suggests a step-by-step approach towards it, through its five maturity levels and provides a detailed guideline for implementing the key processes at each level. It may therefore be worthwhile for a software organization to approach ISO 9000 using CMM as a guideline. It will add value to the ISO 9000 certification by installing a more robust quality system

6. REFERENCES

[1] Quality Systems - Model for quality assurance in design, development, production, installation and servicing. ISO 9001:1994.

[2] Quality Management and Quality Assurance Standards - Part 3: Guidelines for the application of ISO 9001 to the development, supply and maintenance of software. ISO 9000-3:1991.

[3] Quality Management and Quality System Elements - Part 1: Guidelines. ISO 9004-1: 1994.

[4] Paulk M.C. et al., "Capability Maturity Model V1.1", Tech. Report CMU/SEI-93-TR-24, Software Engg. Inst., Carnegie-Mellon Univ, Pittsburgh, 1993.

[5] Paulk M.C. et al., "Key Practices of the Capability Maturity Model V1.1", Tech. Report CMU/SEI-93-TR-25, Software Engg. Inst., Carnegie-Mellon Univ, Pittsburgh, 1993.

[6] Robert C. Bamford and Willium J. Deibler II, Comparing, contrasting ISO 9001 and the SEI capability maturity model, IEEE Computer, October, 1993.

[7] Carl Dichter, Software Audits, UNIX Review, October, 1993

[8] Paulk M.C., "A Detailed Comparison of ISO 9001 and the Capability Maturity Model for Software", (submitted to) IEEE Software.

[9] Radice et al., "A programming process architecture", IBM Sys J. 24(2), 1985.